D:A4.1 Socio-economic impact assessment

Niezen, Maartje; van Woensel, Dominique; Nunez, David; Fernandez-Gago, C; Adams, Samantha; Bjørkvoll, Thor; Frøystad, Christian; Halverson, Trond; Haugset, Børge

Publication date:
2016

Document Version
Publisher's PDF, also known as Version of record

CLOUD ACCOUNTABILITY PROJECT

D:A4.1 Socio-economic impact assessment

Deliverable Number	D14.1
Work Package	WP14
Version	
Deliverable Lead Organisation	TiU
Dissemination Level	Choose an item.PU
Contractual Date of Delivery (release)	31/03/2016
Date of Delivery	29/04/2016
Status	**Final version**

Editor

Maartje Niezen (TiU)

Contributors

Maartje Niezen (TiU), Dominique van Woensel (TiU), David Nuñez (UMA), Carmen Fernández-Gago (UMA), Samantha Adams (TiU), Thor Bjørkvoll (SINTEF), Christian Frøystad (SINTEF), Trond Halvorsen (SINTEF), Børge Haugset (SINTEF)

Reviewers

Siani Pearson (HP), Simone Fischer-Hübner (KaU)

SEVENTH FRAMEWORK PROGRAMME

Revision table

Version	Date	Author	Change Description
0.1	20/01/2016	Maartje Niezen	Document created
0.2	23/02/2016	D. Nuñez	Section on Security Threat Analysis
0.3	14/03/2016	M.Niezen	Adjusted outline
0.4	15/03/2016	M.Niezen	Added Base Case Scenario Adjusted the outline a bit more
0.5	21/03/2016	M.Niezen	Combined and integrated various separate chapters (TiU, SINTEF) into this deliverable
0.6	29/03/2016	M.Niezen	Included scenarios
0.7	30/03/2016	M.Niezen	Included recommendations
0.8	31/03/2016	M.Niezen	Address review feedback, incorporate updated chapter 2 by SA, include references, update captions of figures, include executive summary (SA)
Version 1.0	29/04/2016	M.Niezen	Included feedback and input by Samantha Adams, included data analysis of online questionnaire.

Executive Summary

Emerging cloud ecosystems can potentially have significant impact on individuals, business and society. Because the impacts of these ecosystems can be both positive and negative, they must be developed in a socially robust and responsible way. A key aspect of such development is creating **accountability** for data governance in the cloud environment, as it is a critical prerequisite for retaining control of corporate and private data processed by cloud-based IT services. The Accountability for Cloud (A4Cloud) project takes an interdisciplinary approach to analysing the notion of accountability, and specifying building blocks for accountability. A4Cloud focuses on the question of how cloud (and other) service providers can be accountable for how they manage **personal, sensitive and confidential information** 'in the cloud'?

Part of A4Cloud was devoted to developing accountability measures. This deliverable describes the development a socio-economic impact assessment (SEIA) of these accountability measures and their main features. It also provides a socio-economic impact assessment (SEIA) that aims to inform post-project exploitation strategies in terms of the socio-economic acceptance (e.g. perception of enhanced trustworthiness, value for money, market segmentation, etc.) of these accountability measures in cloud ecosystems. Although many SEIA's are conducted as a part of an environmental impact assessment (EIA), few SEIA's have been conducted on cloud infrastructures and there are no known SEIA's related to accountability measures. As part A4Cloud it was therefore necessary to develop a SEIA specifically adjusted to cloud infrastructures. The proposed SEIA approach in this deliverable builds on earlier work conducted in the WP on the socio-economic context of accountability in the cloud (WP:B-4).

Chapter 1 provides a brief introduction to and definition of the problem. It also outlines how this deliverable is related to other documents from the Accountability for Cloud project.

Chapter 2 describes the approach taken in this work package to developing a SEIA-methodology tailored to cloud ecosystems. A three-step methodological approach was used to develop the adjusted SEIA: an interdisciplinary literature review to identify key methodological aspects and content factors in such assessments, an online questionnaire targeting cloud customers, cloud auditors and cloud providers and semi-structured interviews with cloud users and cloud service providers. The literature review revealed three primary challenges in applying general SEIA methodological approaches to the specific case of cloud computing. First, SEIAs comprise a broad range of methodologies. Notably, many papers adopt a SEIA methodology that focuses either on the economic perspective or on the social perspective, but not on both combined (although they did draw conclusions on both). Which aspect was dominant (emphasized) in the analysis tended to influence the method of choice. Second, many SEIA's are conducted as a part of an environmental impact assessment (EIA). Cloud computing is sufficiently different from the types of technologies included in EIA, whereby elements that are typical for a SEIA as a part of an EIA are not applicable to the case of cloud computing and vice versa. A third, and related, challenge is that there is a dearth of literature on cases of SEIA's describing cloud computing or a very similar topic.

Developing a SEIA specifically tailored to cloud ecosystems therefore requires drawing not only on standard methods for social and economic assessment but also on additional theoretical frames. In this case, we used the Technology Acceptance Model (TAM), which focuses largely on individual acceptance of technologies and the Diffusion of Innovations (DoI) Model, which examines factors that contribute to initial acceptance of a technology and, subsequently, how they 'diffuse' in a given social setting. Using insights from these models reveals three key concepts that shape social and economic accountability: trust, control and transparency, which relate both individually and collectively to the notion of accountability as developed in the C2 framework. Understanding the interplay between these and other factors requires an interdisciplinary approach to understanding acceptance (e.g. value for money, market segmentation, etc.) of given technologies in specific settings.

The SEIA conducted here, supplemented by aspects from theories regarding diffusion of innovations and technology acceptance, provides insights regarding factors contributing to or detracting from acceptance of accountability measures in cloud ecosystems. For the economic methods, we argue that four types of methods are best suited for the SEIA of cloud computing, namely the Cost-Benefit Analyses (CBA), The Input-Output analyses (IO), the General Equilibrium (GE) methods and the Multi Criteria Analyses (MCA). However, in practice the prototype status of the A4Cloud accountability tools prohibited actual conduct of these recommended methodologies. For the social methods, we took into consideration the distributed nature of the cloud, whereby the community of relevant stakeholders

comprises an interest-based, rather than geographically situated group. The best approach for this case of cloud computing is therefore secondary data analysis, followed by a questionnaire combined with interviews validating findings from secondary data analysis.

The chosen combination of economic and social assessment methods, complemented by factors from two technology-specific theoretical models enable a thorough examination of the interplay between three key concepts (trust, control and transparency) in relation to accountability of the cloud. This enables a better understanding of potential implications and allows for assessing plausible alternatives that work better for one group or another.

Chapter 3 defines the "base-case scenario", which is an important starting point for any SEIA. This scenario sketches the current context ("landscape") of the proposed change. The socio-economic landscape defined in WPB4 (specifically deliverables D24.1 and D24.2) was used to develop this scenario. This scenario reflects five key aspects of cloud computing anno 2013. First, cloud computing was introduced and promoted with promises of flexibility and agility at low cost. Second, cloud computing was expected to change the organization and business of society, with the main drivers being economics and increased digitalization in all social sectors. Third, governance of cloud computing had a wide scope largely dominated by the market modality, implying a liberal approach to innovation. Governance via techno-regulation, such as privacy by design, was still in an infant stage in the domain of cloud computing. Accountability frameworks were evolving in relation to changes in technical, but also legal and economic, governance structures. A fourth element was the increase in occurrence of various incidents that raised government and business awareness for the importance of more data protection and security in the cloud. These incidents showed that data management was not only about an individual's responsibility to control his/her own data, but also other actors' responsibility to secure the interface. The fifth and final element was the clear lack of general public/social interest in data protection in the cloud, despite there being more attention for the issue after the aforementioned incidents.

These elements of the base-case scenario revealed a discernible mismatch between the existing and desired cloud computing landscape. Specifically, the socio-economic impact of accountability in the cloud ecosystem was, at that time, reasonably low.

Chapter 4 provides an oversight of the key findings of the SEIA, both on a specific tool level and more generally. These findings were derived from a combination of the individual interviews and the questionnaire results. Most respondents indicated that while they liked the idea of the prototype accountability tools, the descriptions provided were too scientific and difficult to understand. They could not see the overarching need for such tools. Both cloud service providers and cloud customers indicated that they liked the generic focus of the tools, yet they questioned whether implementation was possible. Specifically, because demands can vary greatly per type of organization (public/private sector, type of data involved), they expected generic tools to require significant adaptation to make them fit (and be usable in) that specific context.

More generally, respondents felt that the tools were unlikely to lead to significant cost reductions for the cloud customers. Specifically, they indicated indicate the time and work that would be required to implement accountability, not only the tools but also the entire 'code of ethics' anchoring and governing this process. Nevertheless, they expected the main features of the A4Cloud accountability tools to help out in demonstrating accountability in the near future. On the whole, respondents expressed great interest in the A4cloud project and could see how the tools would be helpful for their own organizations and could add value for both cloud customers and cloud service providers. As expected, the participants differed somewhat in which tool they thought was most valuable. This difference can be attributed to the role that the subject had in the cloud service value chain. The main point of disagreement that we encountered concerned the timing of the project with respect to the market's willingness to pay for increased accountability. Despite some differences of opinion, depending on type and size of the organization they were from, the respondents generally agreed that active enforcement of the new GDPR was necessary for fostering more accountability in the cloud ecosystem.

Chapter 5 contains a security threat analysis for the accountability tools. The security threat analysis helps the SEIA identify and understand both existing risks and new risks that might arise. These individual security threat analyses identify the risks related to the adoption of A4Cloud tools. They identified threats according to six possible attacker goals in targeting data: spoofing, tampering, repudiation, information disclosure, denial of service and elevation of privilege. These could be identified for each tool taking into consideration the dependencies, entry points, assets and trust

levels. This enabled making an estimation of likelihood (unlikely, likely, very likely) and impact (not critical, significant, critical). Combining these led to a matrix that showed the risk of the threat ranging from low (e.g. unlikely and not critical) to medium (e.g. likely and significant) to high (e.g. very likely and critical).

The seven assessed tools reflected a majority low risk score (64%), with a 24% risk of medium threats and 12 % risk of high threats. This was because the impact was low or the threat was unlikely. Three threats were rated as high-risk, related to spoofing, which allows access to crucial aspects such as data subjects' data). Several of the medium risks were also of this type, suggesting the need for proper countermeasures for specifically this type of threat. Such countermeasures would include multi-factor identification and strong password policies. The tools did not add any significant representative threat to interested stakeholders and actually provide accountability and data protection functionalities.

Chapter 6 describes three "near future" scenarios (approximately 3 years from now) for accountability in the cloud allowing for comparison between the base case scenario and the three scenarios. Such alternative scenarios, which are fictional narratives that try to anticipate ethical, legal and social dynamics, are also an important part of a SEIA because they help researchers anticipate the likely acceptance of e.g. a given accountability tool, explore the dynamics of interaction between current morality and new technologies, and outline relevant governing mechanisms.

The first scenario anticipates a situation where there is awareness for the issue of accountability in cloud computing, reflected in discussions at various levels and in various sectoral arenas throughout society. However, there is very little concrete action being taken on the basis of these discussions. In this scenario, implementation of the GDPR has been finalized, yet European and national data protection authorities have received few resources to enforce this legislation. Technological developments that support accountability, such as the A4Cloud tools, have not been recognized and taken up as a lucrative business model. Most accountability tools fail to meet both sector-specific implementation criteria and general feasibility. Though their general functionality is appreciated, the main governance mechanism driving the cloud computing industry remains the market and the related strive for innovation with few legal restrictions.

The second scenario anticipates a moderate degree of discussion and action, related to the two-year implementation phase following enactment of the GDPR. Many cloud stakeholders were encouraged to use the implementation phase for establishing minimal requirements necessary for complying with the regulation, but are finding that it takes more time than two years. Especially enterprises and CSPs that are not digitally native struggle with how to combine the old and the new IT infrastructures within their companies. As a result, the cloud ecosystem has not fully adopted the accountability notion as intended by the A4Cloud project, but organizational changes and adaptation of IT infrastructure towards more transparency about data whereabouts has become the norm. In this scenario, the driving force in the socio-economic landscape remains the market governance mechanism and its push for innovation, yet increasingly the importance of guidelines and frameworks within the cloud ecosystem are recognized.

The third scenario anticipates a high degree of both discussion and action. In this scenario, high-profile incidents such as data leaks and privacy-infringing activities have raised public awareness of the importance of security and accountability in the cloud. Both the public and private sectors have taken 'best practices' for responsible data stewardship. Some companies that started modifying their practices early (i.e. prior to the enactment and implementation of the GDPR) have already started to profit significantly from their reputation as trustworthy CSPs or cloud customers. With increased awareness, technological innovations (such as accountability tools that enable auditing according to GDPR regulations) support a more accountable approach to data handling in the cloud. The market mechanism governing cloud computing is now interacting with other mechanisms such as law and social norms, balancing the drive for innovation with regulations for proper data handling and a responsiveness to societal and customers' demands. Based upon these different impact scenarios it becomes possible to identify mitigation strategies for potential adverse impacts and further monitoring and management of desired impacts.

Chapter 7 focuses on how to proceed with the developed A4Cloud framework and tools in the near future. Both the responses to the questionnaire and interviews and the scenarios outlined in chapter 6 indicate areas where the acceptance of accountability in the cloud ecosystem can be further stimulated and how this can be done. These are therefore used as the basis for six concise recommendations for facilitating more accountability for data management in cloud ecosystems:

1. Provide a stronger legal base for and enforcement of data protection and accountable behaviour
2. Facilitate independent auditing of responsible data stewardship
3. Increase public awareness of the need for accountability
4. Balance existing information asymmetries via partnerships
5. Focus on larger enterprises working in the public sector first, as these can serve as an example for other types of businesses.
6. Demonstrate how A4Cloud tools and mechanisms can be turned into a business model in order to encourage greater uptake and use.

Table of Contents

1 Introduction

1.1 Definition of problem and purpose

The A4Cloud project takes an interdisciplinary approach to analysing the notion of accountability, and specifying building blocks for accountability. A4Cloud acknowledges that **accountability** is a critical prerequisite for effective governance and control of corporate and private data processed by cloud-based IT services. A4Cloud focuses on the question of how cloud (and other) service providers can be accountable for how they manage **personal, sensitive and confidential information** 'in the cloud'?

This deliverable describes and analysis a socio-economic impact assessment (SEIA) of the accountability measures and their main features developed within the Accountability for Cloud (A4Cloud) project. The SEIA aims to inform post-project exploitation strategies in terms of the socio-economic acceptance (e.g. perception of enhanced trustworthiness, value for money, market segmentation, etc.) of these accountability measures in cloud ecosystems. Moreover, the deliverable is in line with the fourth main objective of the A4Cloud project: i.e. **to provide recommendations and guidelines** for how to achieve accountability for the use of data by cloud services, addressing commercial, legal, regulatory and end user concerns and ensuring that technical mechanisms work to support them.

Traditionally when we ask the question whether organisations have some inherent interest in accountability, a list of supposed drivers emerges, which includes [1]:

- Compliance with legal obligations,
- Fear of reputational damage from accountability-related failure in a specific domain (privacy, security, environmental, etc.),
- The need to generate trust with the clientele, and
- Promotion of a good corporate practice.

However these drivers apparently are not all present, since accountability does not yet seem fully embraced by the cloud ecosystem. Therefore the SEIA research described in this deliverable focuses on the likely acceptance and usage of specific accountability tools and their main characteristics more generally.

The main research question guiding the SEIA of accountability in the cloud has been:

How and under what conditions will individual and organizational users adopt accountability tools in general and A4Cloud tools, mechanisms and attributes in particular?

1.2 Relationship to other A4Cloud documents

This deliverable documents the socio-economic impact assessment of A4Cloud as is discussed in more detail in Chapter 2. The proposed SEIA approach in this deliverable builds on earlier work conducted in the WP on the socio-economic context of accountability in the cloud (WP:B-4). WP:B-4 has reported on the need for accountability, cloud stakeholders' behaviour and the requirements for governing accountability in cloud ecosystems taking into account the characteristics of cloud computing from the perspective of socio-economic and ethical considerations. That analysis provides the foundation, especially in the form of a base-case scenario (see chapter three) for determining their impact in this specific WP (WP:A-4). Moreover, WP:B-4 offers the application of economic governance theory to cloud computing (to create different regulatory models to steer responsible stewardship), the study of the willingness of users to pay for accountability services, the modelling of the economic value of accountability services to EU businesses/SMEs (and how a competitive advantage can be gained), the assessment of the economic value of accountability to the public and the demonstration of the value of ethical accountability for sustainability and the health of the cloud ecosystem. Given WP:B-4's focus on economic modelling in more generalised cases not targeted at usage of specific tools, this WP primarily focuses on the SEIA of specific accountability tools.

The study for this deliverable also builds on the work conducted in WP:C-2. Especially accountability's key features as defined in the conceptual framework and as operationalized in the accountability tools play an important role. Subsequently, analysis of the relevant tools also warrants careful consideration of these various key features.

1.3 Structure of the document

The remainder of this document is structured as follows:

Chapter 2 discusses the SEIA-methodology based upon a literature review of existing practices. The chapter demonstrates the challenges faced by the research team and chosen solutions

Chapter 3 defines the base-case scenario

Chapter 4 provides an oversight of the findings of the SEIA both on a specific tool level and more general key findings that can be derived from both the individual interviews and the questionnaire results.

Chapter 5 contains a security threat analysis for the 7 different accountability tools. These security threat analyses identify the risks that already deployed-service and organizational-best-practices, and to assess the impact of such risk upon them.

Chapter 6 describes three near-future scenarios (2-5 years) for accountability in the cloud allowing for comparison between the base case scenario and the three scenarios.

Finally, in chapter 7, a concise set of guidelines and recommendations outlining the socio-economic impact of the projects results will be produced.

1.4 Glossary of acronyms / abbreviations

A4Cloud	Accountability for Cloud and Future Internet Services
AAS	Audit Agent Systems
APEC	Asia Pacific Economic Cooperation
CBA	Cost-Benefit Analysis
CEA	Cost-Effectiveness Analysis
CISO	Chief Information Security Officer
COAT	Cloud Offering Advisory Tool
CORAS	Risk Assessment of Security Critical Systems
CSA	Cloud Security Alliance
CSC	Cloud Service Customer
CSP	Cloud Service Provider
CEO	Chief Executive Officer
CTO	Chief Technology Officer
DoI	Diffusion of Innovations
DoS	Denial of Service
DP	Data Protection
DPIAT	Data Protection Impact Assessment Tool
DPPT	Data Protection Policies Tool
DT	Data Track
ECP	Electronic Commerce Platform (NL)
EIA	Environmental Impact Assessment
ENISA	European Union Agency for Network and Information Security
EU	European Union
GDPR	General Data Protection Regulation
GE	General-Equilibrium
IA	Impact assessment
ICT	Information Communication Technology
ID	Identification
IMT	Incident Management Tool
IT	Information Technology

IO	Input-Output
LE	Large Enterprise
MCA	Multi Criteria Analysis
NSA	National Security Agency (USA)
NIST	National Institute of Standards and Technology
OECD	Organization for Economic Cooperation and Development
OWASP	Open Web Application Security Project
PRISM	Surveillance program by the American NSA
QALY	Quality-adjusted Life Years
RoI	Return on Investment
RRT	Remediation and Redress Tool
STRIDE	Spoofing, Tampering, Repudiation, Information disclosure, Denial of Service, Elevation of privilege
TAM	Technology Acceptance Model
TL	Transparency Log
TiU	Tilburg University
SEIA	Socio-economic impact assessment
SME	Small and Medium Enterprise
SIA	Social Impact Assessment
STAR	Security, Trust & Assurance
UMA	University of Malaga
WP	Work Package

2 A4Cloud's approach to the SEIA of accountability in the cloud

A fundamental premise of A4Cloud is that emerging accountable cloud ecosystems, with their potentially large impacts – both positive and negative – on individuals, business and society, must be developed in a socially robust and responsible way. This implies the need for a comprehensive scope when developing policies, incentives and regulations to govern the accountability of data use within these ecosystems. This WP addresses the role of Socio-economic Impact Assessment (SEIA) herein.

Impact Assessment (IA), generally speaking, is a broad assessment domain covering various tools to predict the consequences of actions in order to integrate preventive measures in the planning of these actions. Impact Assessment contains a range of different assessment methods, perspectives and tools often found in other advisory domains, as well. However, all types of Impact Assessments share a basic overall procedure. Economic assessments (see section 2.1.4) are common in many technological fields, such as health. These assessments primarily question whether technology-related policy measures (i.e. increased accountability in the cloud) have a positive economic impact in comparison to cases without policy measures. In general, Economic Impact Analysis (EIA) focuses on the economic effects of technologies (changes in the economy due to technological developments) (see section 2.1.4). Social Impact Assessments (SIA) (see section 2.1.5) often include "the process of analysing, monitoring, and managing the intended and unintended social consequences, both positive and negative, of planned interventions (policies, programs, plans, projects) and any social change processes invoked by those interventions" [2, p. 5]. The traditional SIA process is characterized as a pragmatic approach to predicting impacts in a regulatory context, while newer versions tend to emphasize the management of the social aspects of development [3, p. 3].

Socio-economic Impact Analysis (SEIA), the approach used here, combines the social and economic assessments, which are often undertaken separately and employ their own specific methods, within the more general framework for impact assessment. Although some information gained from the social impact assessment and the economic impact assessment are complementary and sometimes overlap, the integrated approach of the SEIA can provide a comprehensive and cost effective outcome, in which information is provided on the potential economic impacts as well as important social values attached to the activity. Such an assessment could collect both qualitative and quantitative data in order to combine, for example, perceptions of enhanced trustworthiness with potential value for money and examine how such perceptions may contribute to e.g. market segmentation. SEIA, therefore, provides insights on possible individual and community attitudes and responses to a given (proposed) change. A SEIA is useful for understanding the potential range and impact of various types of proposed change, and the likely responses of those primarily impacted if such change occurs. This is important for impact mitigation strategies to minimize the negative impacts, while maximizing the positive impacts, of the proposed change. Apart from determining the full range of impacts, like the changes to levels of income and employment, quality of life, etc., it is also important to determine the implications of each particular change. This is important because the impacts of a proposal or policy are distinct from, but also influenced by, the larger context. Therefore, it is important to identify the key sources of impact and also separately identify the impacts that arise from other sources.

Much like general IA, SEIA comprises multiple methodological approaches (further explained below) that are selected per case according to the subject and the scope of the SEIA. In order to describe and analyse the main features of the accountability measures developed within the project and provide a SEIA of these A4Cloud-tools, we conducted a systematic literature review of existing SEIA-methodologies. To the authors' knowledge, few SEIA's have been conducted on cloud infrastructures and there are no known SEIA's related to accountability measures, implying the need for a broad approach in the initial phases of this research. Section 2.1 describes the literature review of existing SEIA-methodologies, including the design and parameters of the literature review (section 2.1.1) and giving an overview of the results of this search (2.1.2). The ultimate aim here is not to develop a SEIA methodology that is applicable to all SEIA topics, but rather one specific to cloud ecosystems. We discuss the general setup of a SEIA (2.1.2.1), followed by specific assessment methods related to economic (2.1.2.2) and social (2.1.2.3) approaches. Section 2.1.3 outlines the resulting recommendations for a SEIA methodology for accountability measures in cloud ecosystems. Whereas

the literature review outlines the desirable SEIA-methodology based upon existing practices, section 2.2 further develops A4Cloud's approach to SEIA of accountability in the cloud by focusing on the likely acceptance of accountability by individuals and organisations and what key features are required for engaging in required trust relationships. Finally, section 2.3 reports the actual methods used to elicit preconditions for acceptance and adoption of accountability in the cloud.

2.1 Literature review of existing SEIA-methodologies

2.1.1 Design and parameters

We conducted a systematic interdisciplinary literature review in order to develop a methodology for socio-economic impact analysis of the accountability measures developed within the A4Cloud-project. We searched English-language articles published between 1980 and 2015. Because of the broad scope of the search and the interdisciplinary approach, seven databases were used: Econpapers, HeinOnline, JStor, Science Direct, Taylor & Francis Online, Citeseer and WorldCat. These databases were selected after scanning the databases available via the Tilburg University Library by looking at the fields these databases contained. As extra verification, this database search was complemented by a web search in Google Scholar and Google.

We searched for articles using keywords, starting broadly by searching for the following (Boolean) combinations and alternative spellings: socio economic impact assessment, socioeconomic impact assessment, "Socioeconomic impact assessment", "Socio-economic impact assessment" and Socio economic AND impact assessment. These variations were used to ensure we included all potentially relevant hits. The database, search terms, use of terms, type of search, hits, potential hits, how articles were scanned, and what was excluded (including reason for exclusion) were documented in an Excel sheet. This resulted in 338 relevant hits, judged by the title and small description of the article given in the database. For a complete overview of initial hits, see the table in the Appendix (section 9).

Literature covering one or more of the following topics was included: execution of SEIA, traditional approaches, components, key aspects, use of different tools, development of tools, traits of SEIA and methods. This enabled outlining variations in how SEIA's are conducted, key components of SEIA's and different tools for conducting a SEIA, resulting a good overview factors for determining a suitable approach for conducting a SEIA on the accountability measures developed within the A4Cloud project. More specifically, the SEIA could address changes in stakeholder perception and potential economic impact resulting from enhanced accountability measures.

2.1.2 Results

The initial search delivered 338 potentially relevant hits. We reviewed article abstracts to assess relevancy and discarded articles containing outcomes of SEIA's or an explanation of the relevance of a SEIA. This narrowed the scope to 118 potentially relevant articles. We downloaded and saved complete texts with abstracts for these articles, scanned the abstracts and discarded articles that only mentioned the outcome or an explanation of the relevancy of the SEIA and articles that either contained mostly an environmental impact assessment or only stated what the impact was. This led to 94 potentially relevant articles. We recorded the titles, authors, abstracts and database they were found in, so that we had an overview of which article was found in which database. We filtered out duplicates resulting in 79 articles. We then conducted a third assessment to select articles that met the inclusion criteria, such as explanation of the methodology or development of tools. Final inclusion/exclusion was discussed between the researchers and resulted in 16 articles that were used to describe the setup of a SEIA (section 2.1.2.1), economic (2.1.2.2) and social (2.1.2.3) methods and develop the framework presented below (see section 2.3).

2.1.2.1 Setup

Before assessing the impacts, certain steps must be taken for a SEIA to be complete. Although there are a variety of methods, the choice of which depends on the particular requirements of the SEIA in question, a SEIA generally involves all or most of the next steps:

a. Scoping the nature and boundaries of the impact assessment;
b. Profiling current impacts of the activity that is assessed;
c. Developing alternative impact scenarios;

d. Projecting and estimating effects of different impact scenarios;
e. Identifying and applying mitigation;
f. Monitoring and managing impacts;
g. Evaluating the impact assessment process [4]–[7]

We briefly describe these steps in the following paragraphs.

In the *scoping* phase (a), the goals and boundaries of the SEIA are determined and the SEIA is focused on key impacts. This phase aims to determine the available time and resources for the SEIA, the nature of the proposal to be assessed, social groups potentially impacted by the (proposed) change, key impacts of interest, extent of available information, potential usefulness of the information, how data gaps can be addressed and the process and methods that can be used for the SEIA [4]. Information collected in the scoping phase can be used to determine the approach and optimal level of community involvement in the SEIA. For the purposes of a SEIA, the term 'community' can be understood in two ways: first, the place-based (geographic) community, and second, the interest-based community, often referred to as stakeholders [4]. Involving stakeholders can have several positive effects. For example, more detailed information gathering and identification of the issues of real concern to the potentially impacted community enables a more meaningful assessment that is targeted to the aforementioned key concerns. Stakeholder participation also enables allowing a range of perspectives about the nature of impacts of particular activities to be expressed and recorded as a part of the assessment, as well as dialogue on controversial issues related to the SEIA. Given the variety of methods, SEIA can range from a technical assessment with no community involvement to a fully participatory approach where information is gathered in partnership with the community. How stakeholders can be consulted is mostly part of the social part of the SEIA and will therefore be further explained in section 2.1.5.

Following the scoping phase, it is important to examine current impacts or effects of the activity that is being assessed, which is done during the *profiling* phase (b). In this phase, the developer is expected to collect and interpret information about the socio-economic environment and context of the proposed development. Interpretation of this information should encompass both past and current conditions and trends. Understanding relevant trends and socio-economic dynamics of the area is essential to predicting the gradation of future change that is likely to occur, as well as how much the proposed development may affect this change. This socio-economic "baseline condition" profiling should identify both the resilient and vulnerable members of the potentially affected communities. Both qualitative and quantitative data are necessary to develop a baseline profile; for example, the following information may be gathered: types of activities that may be effected, who undertakes these activities, when and where; the extent/scale of the potentially affected activities, range of values associated with these activities and historical, regulatory or other factors that have an impact on these activities [4], [7] To assess the total impact that the proposed changes will have, both direct and indirect effects need to be taken into account. Direct impacts are those felt by the people, groups and firms that are directly engaged in the activity that is affected. Examples of social and economic direct impacts are changes to the production output, employment, personal and/or business income and expenses, asset value, domestic or household food resources, working conditions, psychological well-being, social services, social well-being, etc. To assess those direct socio-economic impacts, information and data must be gathered on those identified as potentially affected by the activity, the level and nature of the potential impacts and the range of the potential impacts. The most common methods for primary data collection are surveys, interviews, focus groups, and secondary data analyses [4], [7]. Secondary data analysis may be used to collect initial baseline data and then complemented with primary research to fill in the gaps.

The next two phases include *formulating* alternative impact scenarios (c) and *projecting and estimating* the effects of the different impact scenarios (d). These phases lead to a number of plausible alternative scenarios (based on predictions that are summarized into core social impacts) that should be considered by the SEIA. Core social impacts should include: type and magnitude of impacts, direction and location of impacts, community level impacts and direct and indirect impacts. Those impacts may be presented in tables, matrices or using geographical information systems [6].

Subsequent phases include *identifying and applying* mitigation (e) and *monitoring and managing* impacts (f). First, identification of mitigation is necessary in order to manage, reduce or eliminate adverse impacts on the valued socio-economic components or the public concern. Second, systematic monitoring at different levels enables measuring and/or observing changes, including using indicators to make regular, consistent assessments. Finally, adaptive management enables linking the results of

the monitoring with pre-determined limits of manageable change in order to continually improve policy and practices and learn from development outcomes [7].

The final phase is the *evaluation* of the impact assessment project (g). This is a reflexive phase in which the developers review the SEIA process in order to learn and improve.

2.1.2.2 Economic methods

As stated earlier, although they partially overlap, a distinction can be made between economic and social tools. This section outlines the economic methods and tools that can be used in a SEIA. This does not mean, however, that all tools should be applied in every SEIA; rather, these are options to choose from. Because the method(s) applied will depend on the content and scope of the SEIA, we do not identify a best practice method here, but merely outline the primary methods.

Comparing costs and benefits

1. Cost-effectiveness analysis (CEA) in which costs are determined in a monetary unit while the impacts are measured by a single indicator, typically a unit such as crime rate or blood pressure [8].

2. Multi criteria analysis (MCA) states that each of the various impacts should be expressed in its most suitable metric by using appropriate indicators. With the development of e.g. cloud-based services, most of the impacts, such as impacts on the quality of life, scientific production or technological improvement cannot be expressed or transformed into monetary terms. This means that there is a multi-criteria/multi-dimensional description of the non-monetisable impacts of each assessed project, through the use of a set of appropriate qualitative-quantitative indicators. In some cases, this method is also referred to as 'cost-consequence analysis' [8], [9].

3. Cost-utility analysis is a form of cost-consequence analysis where the outcomes are condensed into a single measure of "utility" (quality of life, well-being, etc.). A commonly used measure is the quality-adjusted life year (QALY). Costs are measured in monetary terms.

4. Cost-benefit analysis (CBA) estimates the ratio (or difference) between the benefits and the costs of an application over a specific time period and spatial dimension. Benefits and the costs that are incurred in the future years are discounted by an appropriate rate [8]. This means that the strengths and weaknesses of alternatives can be taken into account and the costs and benefits of the planned activities can be weighed against each other.

Economic models

5. Economic base model is used to assess the effect of exogenous (external) expenditure on a given area on various scales. These models aim to identify and assess what proportion of regional output or employment depends on exogenous expenditure. Base activities influence the development of the area with a consequent effect on non-base activities. The theory divides the economy into two components, namely the activities that satisfy the demands from outside the region, which is referred to as the export base and the activities that mainly supply goods and services to local residents. In these models, the economic output of an area is divided into the output that is sold outside the area and the output that is absorbed in the area.

6. Keynesian multiplier model is based on the idea that part of the initial investment or income that is spent will lead to more income, employment and prosperity. There are various types of Keynesian multiplier models, such as the regional Keynesian multiplier model, in which the basic model idea is that the initial income injection will be spent in a region and will then generate initial income in that region and because part of the additional income is again spent in the region, the process continues. Additionally, an increase in the regional aggregate demand facilitates a supply side response [10].

7. Input-Output (IO) analysis quantifies the interdependencies between production and consumption among different sectors of the economy. This method can be used at the macro level. It focuses on the input and the output generated by some, or all, industries in a country of region. It is linear, which means that it does not take into account for example temporarily dynamic effects (e.g. price changes) and so-called externalities (e.g. pollution or congestion) [10].

8. General Equilibrium (GE) models**.** This approach relaxes the assumptions that can be made by the IO model by specifying both the demand and supply sides of the economy. These models can be used to explore the system-wide consequences of changes to the supply-side of the economy. They are very flexible, but also relatively complicated to set up. [11]. Both IO and GE methods can capture the economic, social and environmental consequences of a project [11].

Finally, in addition there are a variety of econometric models. These are models that seek to identify the statistical relationship that exists between the various economic quantities belonging to the economic phenomenon that is being studied [10].

2.1.2.3 Social methods

For the social methods, again, there are various primary methods that can be used. For these methods, the same remark can be made as for the economic methods, namely that not all must be used in a given SEIA. Which method or combination of methods is used again depends on the content and scope of the SEIA. The best (combination of) methods for a particular SEIA should be assessed in the scoping phase of the SEIA and depend on, for example, available resources, availability and reliability of relevant secondary data and goal of the SEIA. As above, this overview does not provide a general approach for all SEIA's or identify a best practice method.

1. Secondary data analysis. In conducting secondary data analyses, the researcher collates and re-analyses existing data from a variety of sources, such as papers or reports. The assessment must consider that the original data might have been collected for another purpose, whereby it is potentially unsuitable for the purpose at hand. It may not be possible to identify specific detailed impacts and the data may contain biases which will cause misrepresented impacts if those data are used for different purposes other than those for which it was initially collected [4], [7].

2. Surveys can collect both qualitative and quantitative data, depending on the nature and type of questions asked. Qualitative surveys often use open-ended questions to obtain more descriptive information through a less structured approach, providing a broader range of details and possibly unanticipated or unexpected information. Quantitative surveys are more structured and are framed to allow numerical coding and description of responses. Researchers can use descriptive and analytical statistics to provide general background for a particular situation. Survey results provide a quantitative estimate of public opinion, for example, identifying the key themes among the issues of concern or, estimating users' willingness to pay [8]. In the latter case, the survey helps determine the amount of money that individuals are prepared to pay in order to receive a certain benefit [12].

3. Interviews ask questions to a specific person, such as key experts or stakeholders. Interviews may be held face-to-face manner, over the phone, through skype or via email. They vary from completely structured (much like a spoken survey, where the interviewer does not deviate from the question list), to completely open, where the interviewer gives the respondent free rein to determine the course of the conversation. A common form is the semi-structured interview, which is a mixture of standardized questions and determining additional questions based on respondent answers. Interviews can be used to anticipate reactions or gain key individual support, provide targeted education and gather extensive details, because the interviewer can continue to probe the respondent until the information given in the answers is considered to be complete and sufficient. Interviews can easily be used in conjunction with other methods – an in-depth interview, for example, can be conducted as a follow-up to a previously conducted survey, where the interviewer solicits more detailed information about certain answers given in the survey [5], [9], [13]. Conversely, interviews can be used to identify topics to address with a larger population in a survey.

4. Focus groups (also called group interviews) are small discussion groups, conducted by a professional facilitator, that foster discussions in order to understand the 'typical' reactions of the general public. They may be homogeneous, whereby they gather the opinions of a given demographic group, or heterogeneous, to gain an impression of the position of a broader cross-section of society and there may be several parallel groups or sessions to get more data that can be compared between groups. Group interviews enable in-depth reactions and discussions, whereby the level of input contains a great amount of detail. Analysis of the focus groups can be used to predict the emotional reactions that will rise in relation to the project, but may not be entirely representative of the general public or a specific group. More groups can mitigate this problem of the representativeness [13].

5. Hearings are formal meetings with formal speeches and presentations. They can be used for in introductory or final phases and are useful for legal purposes or to handle the general emotional public input safely. Hearings used at the start of a project provide information to the community so that it is clear what will happen, which can initiate a process of communication between parties. Hearings held toward the end of the project can be used to publicize results, but are generally not intended to collect substantive comments or new data [13]

6. Meetings are less formal than hearings and attendees may present information, but also ask questions, making them more dialogic in nature than hearings. They are generally considered to be a legitimate public forum where individuals and groups can be heard on issues – they may even be structured specifically for this purpose – although the actual legitimacy is sometimes questioned. Meetings may provide more room for informal small group interaction in a less formal setting [13].

7. Workshops are smaller meetings designed to complete a task or communicate detailed or technical information. They are intended to foster a maximum degree of dialogue and can also – importantly – be used for consensus building between stakeholders. Workshops work best with small audiences and several different workshops may be required to reach various stakeholders [13] .

8. Choice modelling is a technique that has been adapted from conjoint analyses (rooted in the transport and marketing sectors) that estimate values in economic research, in order to include social issues. It can be used to examine the trade-offs between economic and social issues or values. Choice modelling involves asking respondents to a survey to make a series of choices about alternative scenarios. Each choice set involves a number of profiles that describe the alternatives on offer. One of those profiles describes a current or future status quo option, and remains constant between the choice sets and this thus gives the respondent a default option in which he or she can choose to keep the current situation. The alternatives mostly offer some improvements to the current situation, but those alternatives imply some monetary cost. The alternatives are described by a set of attributes and variations in the levels of each of those attributes create differences in the choice sets on offer. The main advantages of using this technique in the social field is that it assesses the preferences of the community of interest, focuses attention on the most relevant issues or attributes and provides some quantitative feedback about the relative importance of those issues and attributes [14].

Several of the methods mentioned in the preceding paragraphs can be combined in a small-scale pilot study, whereby the tools that are planned to be used in the SEIA can be tested within a small group. A pilot study can be used, for example, e.g. to check the validity and applicability of a questionnaire, avoid overly abstract notions, ensure the cultural sensitivity of the questions and to practice fieldwork. Based on interviews with the participants of the pilot study, the methods and tools can be adapted, for example by using a questionnaire in which questions can be revised to improve readability and clarity [15].

2.1.3 Recommendations for a SEIA methodology of the accountability measures in cloud ecosystems

Having reviewed the various methodological choices available for performing a SEIA (2.1.2.2 and 2.1.2.2.), we now consider three primary challenges in applying general SEIA methodology to accountability measures in cloud and then outline a plausible methodological combination for conducting a SEIA in this specific case.

The literature review revealed a broad range of methodologies used in SEIAs, making the choice for this particular case especially challenging. Even within articles that could be categorized together, in that they applied a SEIA to the same sector or technological phenomenon, we observed many differences in methods applied. Notably, many papers adopt a SEIA methodology focused either on the economic perspective or on the social perspective, but not on both combined (despite drawing conclusions on both). Which aspect was dominant (emphasized) in the analysis tended to influence the method of choice. In articles where the economic perspective was dominant, researchers tended to use economic formulas to calculate outcomes that they could couple with specific effects that they used in order to draw conclusions regarding economic and social impacts. Conversely, in articles that were dominated by the social perspective researchers used sociological tools such as secondary analysis of existing data or surveys to derive both economic and social impacts. Because the two methods *can* overlap, if one method is used, it does not mean that researchers cannot draw conclusions about the effects of both the social and economic aspects. Indeed, in the reviewed articles, authors tended to draw conclusions on both, which is why we discuss the varied approaches not as absolutes, but as examples of one methodology dominating the other within the overall assessment.

A second challenge was related to the fact that that many SEIA's are conducted as a part of an environmental impact assessment (EIA). For the case of cloud computing, there are no environmental concerns in the traditional sense of this word, i.e. consequential for a specific natural geographical location, which implies that some elements typical to an EIA are not applicable in this case. One

example is the impact on local communities; while there are identifiable communities that use cloud functionalities, in keeping with the nature of the cloud, they are geographically dispersed, which means that the type of potential 'community' influence is not the same as in an EIA, where this refers to, e.g., residential proximity to a project site. Rather, as is identified in section 2.1.2.1, community may refer to those organized around a common interest, or stakeholders. The third, and related, challenge is that the articles we reviewed focused on the research methodology of SEIA's and did not include cases of SEIA's describing cloud computing or a very similar topic. Since there are few known SEIA's on cloud computing and none on accountability, many elements from the literature review will not (always) be directly applicable to a SEIA applied to the cloud. Conversely, cloud computing has specific attributes that may not have been incorporated in prior SEIAs. The scoping phase of the SEIA (as depicted in section 2.2) therefore focuses on the development of a SEIA for cloud, tailored to the specific characteristics of cloud ecosystems.

Recognising the challenges for conducting a SEIA for accountability in the cloud, this project uses a mixture of methods, relying on both primary and secondary data analyses. It is important to note that in the case of accountability measures in cloud ecosystems there are numerous and diverse stakeholders who should be involved in order to achieve an optimal outcome of the SEIA.

Of the economic methods outlined above, we find four well-suited to a SEIA of cloud computing: Cost-Benefit Analyses (CBA), Input-Output analyses (IO), General Equilibrium (GE) methods and Multi Criteria Analyses (MCA). CBA is helpful for determining the costs and benefits of the developed tools in the context of the accountability measures in cloud ecosystems and the costs and benefits of the alternatives, enabling assessment of which tools can best be deployed. IO allows for examining potential effects of the input of a certain cloud computing tool on the output of that sector. GE complements this by relaxing the assumptions made by IO model and including external factor. Finally, MCA is suited to determining the impacts of ICT developments, where many of the impacts are not captured in monetary terms. This method makes it possible to take into account both monetary and non-monetary factors and makes the analysis most complete.

For the social methods, it is important to consider that the two types of communities mentioned in section 2.1.3, namely the place-based/geographical communities and the interest-based communities. Because of the distributed nature of the cloud, interest-based communities are more relevant for a SEIA than place-based communities, which renders specific social methods (such as hearings or workshops, which might not yet be adaptable to an online environment) less effective. The best approach for this case of cloud computing is therefore secondary data analysis, followed by a survey combined with interviews. After secondary analysis gives an initial indication of potential issues, the survey makes it possible to determine this more concretely among the broad range of stakeholders, and allows for an estimation of the user willingness to pay, because some of the developed tools will come at a cost. Moreover, in the survey, the willingness to pay can then be determined for every assessed tool, allowing for a greater degree of comparison. The willingness to pay compliments the question of adoption of the accountability tools by organisations and individuals with insight in the worth of accountability according to its users [16]. Supplementing this with individual interviews enables gathering more detailed information about the reasons and motivations behind the survey answers, which is important for understanding the greater socio-economic implications of accountability in cloud ecosystems.

This selection reveals how context-specific factors lead to practical choices regarding methods (specifically in relation to affected communities). It also shows how combining a limited number of tools nonetheless provides an overview of economic factors and sociological factors, which enables better understanding of why people do or do not accept a given technology and how it diffuses in practice. This leads to a better understanding of which stakeholders emphasize which factors in a given setting or situation and how they explicate or justify the reasoning for why they place importance on one factor or another. This, in turn, provides a better understanding of potential implications and allows for assessing plausible alternatives that work better for one group or another.

2.2 Further development of the SEIA-methodology for accountability in the cloud

As is stated above, the SEIA approach must be specially tailored to accountability measures for cloud ecosystems to assess the impact of some of the tools developed in the A4Cloud project and take into account particular challenges. In this section we determine how to approach the SEIA within the limits (time / resources), the social relevant groups and technologies to study, the expected extent of available information and required (additional) methods for our SEIA-methodology for accountability in

the cloud, i.e. this section represents the scoping phase of the SEIA. Identifying the probable acceptance of accountability tools and mechanisms in the cloud ecosystem, as may be achieved through a SEIA, is a good indicator of the potential impact of the A4Cloud project. What factors contribute to organisations' decisions to introduce accountability tools and mechanisms? The (prototypes of) accountability tools developed within A4Cloud can best be regarded as innovations in cloud ecosystem that aim to improve overall responsible data stewardship within the system. However, to what extent will such tools actually be implemented in cloud ecosystems? When will they be implemented? Theories of technological diffusion and acceptance (see next section) help answer these questions and, when combined with a SEIA, also provide more insight on socio-economic impact.

2.2.1 Additional frameworks related to technological diffusion and acceptance

Two complementary frameworks on technological diffusion and acceptance are especially helpful in relation to cloud ecosystems: Davis' Technology Acceptance Model (TAM) [17], [18] and Rogers' Diffusion of Innovations (DoI) Model [19]. TAM focuses largely on individual acceptance of technologies, while DoI examines their acceptance in organizations in groups – factors that contribute to initial acceptance and, subsequently, how they 'diffuse' in a given social setting.

The TAM focuses on perceived usefulness and ease of use of a given application or tool, attitudes towards using that application or tool, behavioural intention to use and actual system use. Unfortunately, because most of the accountability tools addressed here are still prototypes, actual hands on experience is difficult. Therefore, it is necessary in such cases to use input from this model to try and *anticipate* probable acceptance by focusing on the key features of the accountability tools and asking respondents to react based upon the key features. Both perceived ease of use and perceived usefulness are important factors explaining system use. Because accountability tools do not focus on productivity (i.e. quantity) but on the process of accountability (quality), questions with respect to perceived usefulness do not completely fit the purpose. In a later study, perceived usefulness is related to quality, which is how the attribute is used in this study.

Pavlou (2003) introduces the aspect of trust in the TAM [20]. Trust is a defining feature of most economic and social interactions, especially where uncertainty is present, which is common with new technologies. All interactions require an element of trust, especially interactions and transactions conducted in cloud ecosystems, where the number and type of stakeholders is not always clear. In relation to this project, accountability tools that enhance transparency about cloud providers' characteristics, how verification of compliance is carried out and the degree of user control arguably increase trust in other stakeholders in the cloud ecosystem. Trust therefore incorporates both trust in other parties and trust in the technical infrastructure [21], [22] .

Rogers' diffusion of innovation (DOI) model also provides key aspects relevant to the case of cloud computing [19]. Namely, this enables considering how an organisations' reason to use accountability tools is potentially different from a given individual's underlying reasons for adoptive behaviour. Whereas individuals' adoption choices can best be studied via the decision making process leading to the utilization of an innovative tool or mechanism, an organisation must, according to Rogers, pass through five different stages in an organisational process of innovation adoption: a) agenda-setting, b) matching, c) redefining/restructuring, d) clarifying and e) routinizing.

Rogers distinguishes two different categories of variables that influence the process of innovation diffusion in organizational settings: a) the characteristics of the innovation itself and b) internal and external characteristics related to the organisations. Internal organizational characteristics refer, for example, to the size and type of the organization, management attitudes toward a technology or aspect thereof, degree of concentration for decision-making within the organization, level of bureaucracy and degree of openness. External organizational characteristics are about the greater socio-economic context and refer to e.g. legislative pressure, sectoral norms (such as regarding data protection) and relationships with other public or private organizations. Also in this model trust and transparency play a role (evident, for example, in the importance of the degree of openness and attention for how decision-making is structured, as well as how control over various processes is determined) [23] (see also next section 2.2.2).

2.2.2 Trust, control and transparency

In the additional frameworks, three key concepts relate both individually and collectively to social and economic accountability: trust, control and transparency. The adoption of cloud computing services by cloud consumers is greatly affected, for example, by customers' trust in cloud computing [20], [23]–[25]. This trust is shaped by customers' perceptions of risk in cloud providers and their services. However, risks are perceived differently by different stakeholders. Privacy statements, security policies and risk assessments are some of the methods to engender trust to cloud providers' services.

This is related to control because one of the governing mechanisms of control is setting standards to which relevant stakeholders must adhere. Standards are used to regulate behaviours and practices, promote (socially) desirable actions and dissuade (or forbid) undesirable actions. Demonstrating increased control over personal data may encourage usage of CPs services/platforms infrastructure, which if tied to chargeable service, could provide financial benefit. However, risk assessments, especially, but also security policies, should be dynamic and "on-demand". Moreover, they should address cloud consumers' concerns: e.g. privacy intrusions, availability of services, usability. This, in turn is related to transparency. Having insight in processes and decisions allows cloud subjects and cloud customers to make informed decisions. The free exchange and access to information, including the evidence and reasons behind decisions, are considered to be of high value.

Cloud subjects and customers have a right to expect that institutions or organizations they trust will share with them the information necessary to make informed decisions, such as whether (to continue) to use a cloud service or not. When cloud subjects and customers trust others, they expect these others to control information disclosure in their interests. Nondisclosure of information to protect their own interests or to hide conflicts of interests potentially erodes trust. Since not all stakeholders need full disclosure of all types of information available, trusted parties can be responsive to publics' needs for transparency and disclosed information.

Because trust, control and transparency shape social and economic accountability at multiple levels and are relevant to all stakeholders (and the relationships between them), the theoretical frame or model that guides the impact assessment of A4Cloud tools and mechanisms must include these three concepts and attempt to understand the interplay between them [26], [27]. In order to study the socio-economic impact of A4Cloud's introduction of the accountability notion in the cloud ecosystem, we therefore focus on the factors contributing to the adoption of accountability. In other words, to what extent will cloud accountability tools enhance trust, control, and transparency in responsible data handling, collection, processing according to their (potential) users? To what extent do/will (potential) users adopt such tools because of these trust, control and transparency enhancing features? Understanding the interplay between these and other factors requires an interdisciplinary approach to understanding acceptance (e.g. value for money, market segmentation, etc.) of given technologies in specific settings. The SEIA conducted here, supplemented by aspects from theories regarding diffusion of innovations and technology acceptance, provides insights regarding factors contributing to or detracting from acceptance of accountability measures in cloud ecosystems.

2.3 A4Cloud's SEIA research methods

We used a combination of a questionnaire distributed to SMEs and cloud providers based upon the model above, semi-structured interviews with experts and stakeholders using a topic list based upon the frameworks on technological diffusion and acceptance, and secondary data analysis of reports on cloud adoption and the need for accountability and/or data protection. Specifically, we focused the questionnaire on the prototype accountability tools developed within the project, which made the topic more tangible for respondents.

Because both time and chosen methods (online questionnaire and semi-structured interviews) did not allow for exploring all 12 prototype tools, we selected 7. In section 2.3.1 we explain how we delimited the exploration of the A4Cloud Accountability tools to 7 prototypes. Our focus has been on eliciting and describing the potential of the tools and their likely acceptance in cloud ecosystems and the likely acceptance of key accountability features: control and transparency, information and compliance. In order to study the seven tools' potential and likely acceptance of accountability's main features we initially intended to use three methods:

- An **online questionnaire** amongst end users, cloud customers, cloud auditors and cloud providers (N=206) (see section 2.3.2)

- Semi structured **interviews** with cloud users and cloud service providers (N=9) (see section 2.3.3)
- Validation workshop – an A4Cloud workshop March 7th 2016, Brussels

Despite extended efforts to find workshop participants (initial recruitment and interest requests for the workshop started at CSA's conference in November 2015), the workshop planned for March 7th 2016 was cancelled, due to lack of participants. Rescheduling was not possible within the remaining project period. The four potential panel members for the socio-economic validation session in this workshop agreed to be interviewed instead.

Section 2.3.2 further outlines the questionnaire's design and distribution process and section 2.3.3 describes our approach for the semi-structured interviews. Finally, section 2.3.4 outlines the analytical approach.

2.3.1 Selection of tools / governance mechanisms to be evaluated

In total 12 tools were developed within the A4Cloud project see Appendix 9.2 for full table and below (Figure 1) for a graphical illustration of the tools and their main characteristics.

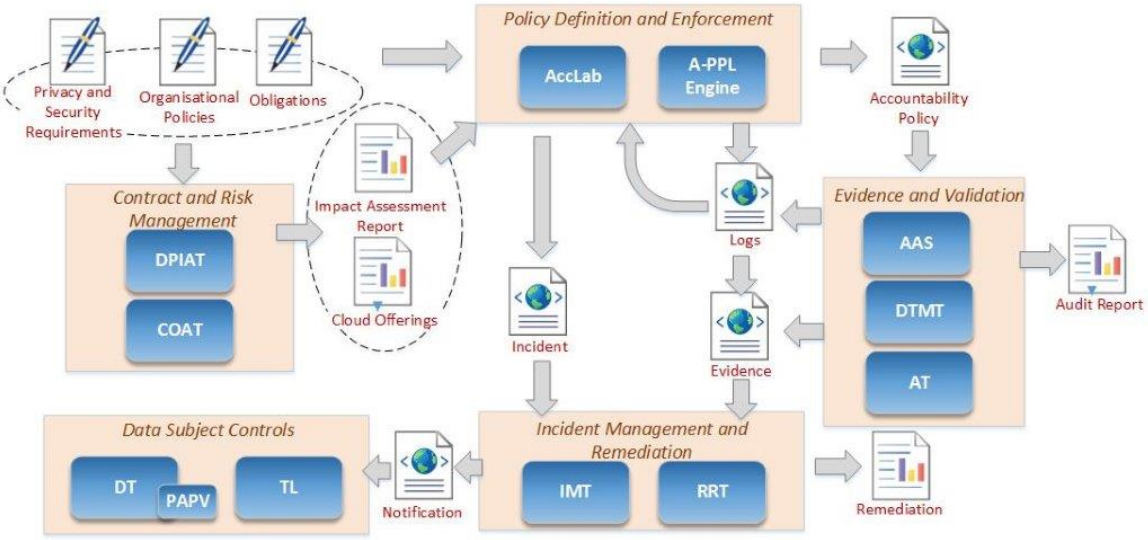

Figure 1 A4Cloud prototype accountability tools in cloud arrangement
Note: A-PPL Engine also depicts the position of the DPPT

As mentioned above, due to time and technological constraints, we selected 7 of these 12 tools for evaluation. This selection was based on the following criteria:

a) all relevant stakeholders represented in the tool selection (i.e. cloud subject, cloud customer, cloud provider, cloud auditor / supervisory authority)
b) all main features of accountability represented in final tool selection (i.e. control & transparency, information / informed consent, compliance), and
c) stage of development (based on availability of pilots / prototypes)

The final tool selection was discussed with A4Cloud project management in a teleconference November 3rd 2015. We selected the following tools; the Data Protection Impact Assessment Tool (DPIAT), the Audit Agent System (AAS), The Data Protection Policies Tool (DPPT), the Incident Management (IMT) and Remediation and Redress tools (RRT) and the Data Track (DT) and Transparency Log (TL) tool. These tools were individually assessed by a SEIA. Note however, that of these 7 tools especially the Incident Management (IMT) and Remediation and Redress tools (RRT) are closely linked. We briefly describe these tools and their application in the use case developed within the framework of the A4Cloud project.

TABLE 1 Selected tools for analysis and their key features

Accountability tool	Key feature	For use by
DPIAT	**Informed choice**	SME (cloud customer)
AAS	**Compliance (evidence)**	Cloud service provider
DPPT	**Control and transparency (**policy definition and enforcement)	Cloud provider implementing policy, cloud customer
IMT	**Compliance (Incident management & remediation)**	Cloud service provider (assess incidents and generate notifications) / cloud customer (individual / organisation)
RRT	**Compliance (Incident management & remediation)**	Cloud subject, cloud customer
DT	**Control and transparency (**Personal data tracking and electronic execution of Data subject access rights)	Cloud subject, cloud service provider
TL	**Control and transparency (**transparency logging)	Cloud subject, cloud service provider

The **DPIAT** identifies risks involved with carrying out a certain business transaction in a given configuration and environment. The tool is used by Small-Medium enterprises (SME's) to assess the classification of the data used in the business transaction and how they can be secured in the cloud. The tool also reports on risks with respect to data breaches and the privacy of the cloud service users. Finally, it also provides insight about potential threats associated with the detected risks. The output of the DPIAT is a report that includes the risk profile document including advice on whether to proceed or not with the specific business transactions and the suggested mitigations in cases of risk exposure. The tool logs the offered advice and the users' decision regarding accountability purposes and also educates the user on risks and threats to ensure the ethical aspects of accountability [28].

The next tool is the **AAS**, a tool for auditors and providers that makes it possible to verify the compliance with custom policies. It enables the automated audit of multi-tenant and multi-layered cloud applications and cloud infrastructures to comply with custom-defined policies, using software agents. The agents can be deployed at different architectural layers of the cloud with the purpose of collecting and processing evidence, generating audit reports and aggregating new evidence. This tool uses audit tasks in which the data collection sources and tools used to collect data are specified and policies to specify the thresholds and constraints, against which the evidence is examined to generate the audit results [28].

The **DPPT** facilitates the joint specification (cloud customers and cloud providers/brokers/carriers) and implementation of accountability policies by creating a machine readable privacy policy and a technical representation of the policy. This machine readable policy allows for the (automatic) policy enforcement of data protection. The policy definition part starts with the specification of the privacy policy. This policy is derived by a Privacy Officer and takes the form of a legal document, which is enforced by an ICT tool (the A-PPL Engine in our case).

Incident Response and Remediation encompasses two tools, namely the Incident Management Tool (**IMT**) and the Remediation and Redress Tool (**RRT**). IMT is the entry point for handling anomalies and detected violations in cloud environment scenarios. This tool receives incident signals and takes the initial steps to respond to these incidents by sending alerts to the users when a relevant incident has occurred based on different parameters. RRT aims to assist individual or small SME cloud customers in responding to (perceived) incidents in their cloud arrangements and is activated when certain incidents are reported by the IMT or when it is invoked by the users on the basis of information collected from other sources, like newspaper reports. If the tool is triggered by the IMT, then the RRT knows what type of incident has occurred, will give the possible actions that can be undertaken and will guide the users through the actions. The tool can also be consulted by the user without being triggered by the IMT, which will result into a dialogue engaged by the RRT with the user to establish their concern and the guide the user through the appropriate actions [28].

Finally, there are the Data Track (**DT**) and Transparency Log (**TL**) tools. The DT is used by data subjects who want an overview of all the personal data they have disclosed. This tool allows them to search through their history of data disclosures to see what personal data they have disclosed, to

whom and under which privacy policy ([28]. The TL is based on the cryptographic scheme Insynd, which is used for secure and privacy-preserving unidirectional asynchronous communication in settings where intermediate servers are considered as active adversaries. Insynd is used to provide a one-way communication channel between service providers and data subjects, enabling a reliable channel for sending notifications to data subjects, even for privacy-sensitive data that normally cannot be sent via email [28].

2.3.2 Online questionnaires

We developed an online questionnaire to assess (perceived) usefulness and user acceptance for the seven selected accountability tools for cloud computing systems. Importantly, the questionnaire embodied the integrated approach of a SEIA (i.e. combining social and economic relevant aspects). While the questionnaire was mainly designed for the social part of the SIA, it also entailed relevant components for the economic assessment, such as expected usefulness of the tools in daily practice, quality, and cost elements. The questionnaire aimed to generate a baseline for the interviews, hence the focus on key features of accountability tools and not on all tools developed within A4Cloud. Respondents were asked to read descriptions of the tools and answer a series of questions regarding trust in the tool and how it addressed issues such as user control over data and transparency regarding data use. This was intended to assess potential user confidence that the tools would comply with their expectations, business policies and regulations. Basic data about the respondents (e.g. position and decision-making capacity within their organization) and the company they represented (e.g. public or private) was also collected.

Initially, the questionnaires were distributed among SMEs and CSPs. The questionnaire was designed in LimeSurvey 2.5. Despite distribution of the questionnaire via the Cloud Security Alliance, requests to A4Cloud partners responsible for developing the tools to distribute the survey in their networks, spread in our own networks and the request of promoting the survey in several associations (amongst which EuroCloud and ENISA), only 25 people accessed the questionnaire, with 8 persons fully filling out the questionnaire. Because validation of interview findings remains important, a final questionnaire was distributed via ‘GlobalTestMarket to a panel that includes respondents who work with cloud services for business purposes. This particular questionnaire was distributed to cloud customers only using LimeSurvey. In total 1204 respondents based either in the UK or in the Netherlands were invited, of which 251 indicated to make use of cloud for business purposes. Of these 251 respondents we deleted 45 due to incorrect answering of a quality control question, resulting in 206 completed questionnaires suitable for analysis (21% response rate – excluding quality control question, 17% response rate, including quality control question).

2.3.3 Interviews

Semi-structured interviews were used to gain understanding of the perceived usefulness of the accountability tools and internal and external characteristics of organisations that might influence likely adoption of these tools. Also, they were used to gain understanding of expected costs and benefits related to the accountability tools. Semi-structured interviews follow a set order of topics, while allowing the interviewer to respond to points raised by the respondent. This adds flexibility to the interview process to allow for unexpected answers, which are important when validating a framework. The validation interviews were conducted face 2 face, by telephone and Skype, and were recorded and transcribed verbatim. In total 9 respondents have been interviewed (TiU: 4, SINTEF:5), with the following characteristics: a) role in the cloud ecosystem: 3 CSPs, 4 CSCs, and 2 cloud brokers, b) size of the organisation: 6 LEs, and 3 SMEs, and c) operating in the following sector: 5 in the public sector, 1 predominantly in the private sector and 3 in both the public and private sector.

Thematic topic lists were developed for both the social impact assessment and the economic impact assessment. For the former the model developed in section 2.2.1 was used to define the topic list (see Appendix 9.4). For the latter the business model canvass of Osterwalder was used as a base for the semi-structured interviews (see Appendix 9.5 for the interview guide) [29].

2.4 Analysis

The analysis of the semi-structured interviews is based upon deductive thematic analysis of the interview transcriptions and minutes. The thematic analyses follow the logic of the topic list (see

appendices 9.4 and 9.5). We made use of IBM SPSS descriptive statistical analysis of the online questionnaire data.

3 Base-case scenario

In the base-case scenario information about the socio-economic environment and context of the proposed development, introduction and acceptance of accountability tools in the cloud is provided according to the profiling phase of the SEIA. The base-case scenario depicts socio-economic landscape of the cloud ecosystem at the start of the A4Cloud project. Understanding the socio-economic landscape of cloud computing is essential to predicting the gradation of future change and the likelihood that accountability will be part of this change. In this SEIA we will depart from the socio-economic landscape as defined in WPB4, specifically deliverables D24.1 and D24.2 describing the socio-economic landscape as investigated between 2012 and October 2014 [30], [31]. A socio-economic landscape can be defined as a framework containing the relevant social and economic factors explaining the behaviour of relevant stakeholders within the cloud ecosystem. This research also provides a good base-case for current assessment of the socio-economic impact of accountability in the cloud now and in the near future.

3.1 The socio-economic landscape of accountability in the cloud anno 2013

Based upon a literature study (white papers on cloud characteristics, benefits and concerns, academic literature on cloud adoption and cloud security, and (online) newspaper articles reflecting societal movements) deliverable D24.1 describes the identified social and economic factors explaining cloud stakeholders' behaviour in the (preliminary) socio-economic landscape[1] of cloud computing:

a) The ideal of cloud computing,
b) The drivers of cloud computing,
   Current governance of cloud computing,
c) Incidents that make problems with cloud computing visible,
d) Society's interest in cloud computing, and
e) Security in cloud computing.

This identified socio-economic landscape of cloud computing provided an initial framework to explore the status in cloud computing with regard to accountability, trust, transparency, control and other relevant notions that define responsible stewardship in the cloud. The socio-economic research concluded that the existing socio-economic landscape at the start of the A4Cloud project was not yet ready to embrace the accountable cloud computing landscape envisioned by the project. In fact, the socio-economic impact of accountability in the cloud ecosystem can be regarded as reasonably low by the end of 2013.

Cloud computing has been introduced and promoted with **great promises of flexibility and agility** at low cost [32], [32]–[34]. In addition the NIST (National Institute of Standards and Technology) definition of cloud computing seems to confirm cloud's advantages in its definition of the cloud's key characteristics: "on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service" [35].

These promises of cloud computing are also embraced by society at large. Cloud computing is deemed to **change society's organization and business**. Two main drivers of the cloud are: a) economics and b) society's (forced) digitalization. First, cloud computing's economics refers to utility computing over conventional hosting. The introduction of cloud computing and big-data has changed business models to focus not only on money, but also on data. Data is the so-called 'new oil' has become a commercial and tradable asset. According to Etro (2009) cloud will have a positive impact on entry and competition in all sectors where fixed ICT spending is crucial [36]. Secondly, cloud computing embodies the digitalization of society and enforces organizational (new ways of living our lives, perform work, do business and administer public tasks and services) and societal changes (towards a 'better' society) [37]. Both drivers of cloud computing provide an explanation of how cloud computing will lead / leads to a fundamental shift in the organization of society and business. Accountability and/or accountable behaviour are not yet part of the cloud's main drivers.

[1] A socio-economic landscape is defined as a framework containing the relevant social and economic factors explaining the behaviour of relevant stakeholders within a specific ecosystem [30].

Governance, as understood as element of the socio-economic landscape of cloud computing has a wide scope: ranging from law to other modalities regulating cloud computing such as the market, social norms and techno-regulation or code [38]. Late 2013, the governance of cloud computing largely is dominated by the market modality, implying a liberal approach to innovation. In order for the innovative cloud to flourish, one should let the market regulate. Yet, simultaneously, the notion of accountability is already enshrined in various regulatory and legal frameworks for data protection across the globe, notably the Organization for Economic Cooperation and Development (OECD) privacy guidelines [39], Canada's Personal Information Protection and Electronic Documents Act (2000)[2] and Asia Pacific Economic Cooperation (APEC)'s Privacy Framework [40]. Accountability concepts are evolving as the current legal framework responds to globalization and new technologies, and indeed the forthcoming revision of the EU Data Protection Directive includes this concept. Less prominently visible is the regulation of cloud computing via social norms. Accountable behaviour is shaped in the relation between cloud consumers and cloud providers too and requires, for example, some margin for self-governance by cloud providers[3]. Since cloud computing forms an essential part of global critical infrastructure, responsiveness to societal input on its governance might be relevant as well.

Last, governance via techno-regulation, such as privacy by design, is still in an infant stage in the domain of cloud computing. However, previous EU projects, such as Prime and its follow-up PrimeLife, have already focussed on privacy enhancing technologies and can provide guidance for A4Cloud in steering towards responsible data stewardship by means of embedding privacy by design in cloud supporting tools.

Another element defining the cloud's socio-economic landscape has been the occurrence of various **incidents** raising public but also business' awareness of the need for data protection and security in the cloud. From a societal perspective Snowden's unveiling of NSA's surveillance practices via PRISM has played an important role in stimulating the 'privacy' debate, even though the case did not have a direct connection to cloud. In addition, the increased distrust in the American intelligence has led to speeding up the process of enacting laws on privacy and surveillance in, for example, Brazil.

The focus on the extent of control one has on your own information became, for laymen, an important issue. In contrast, from a business perspective, these incidents however also demonstrated a different side to cloud, the one in which its **security** has been emphasized. Increased knowledge and awareness about security and the cloud has changed business attitude from initial fear and reluctance to increased confidence and willingness to integrate cloud. This does not mean security is no longer an issue, yet has become less prominent and discussions of security issues have become more mature in nature.

A last element defining 2013's socio-economic landscape is the **societal interest in cloud computing** in relation to data protection, or better said the lack thereof by the public at large. Despite the increased awareness of privacy concerns, laymen's interests in the risks that come with IT innovations are rather low. Yet, simultaneously, governmental bodies and public institutes have raised the need for governing innovation in a responsible manner. Articulation of the public issue at stake with cloud computing might not be a self-evident matter, yet a better understanding of what the public wants and needs is necessary to warrant for responsible innovation. Especially since it is questionable whether the drivers of the innovation, i.e. cloud computing, can be trusted to act responsibly, when they are deemed to do so and how the public will know they do. Hence responsiveness towards the public's cloud computing concerns, whether they are related to uncertainty of knowledge or the cloud's social and ethical impacts, is necessary for future responsible development of cloud and future internet services. The 2013 cloud computing landscape, however, depicts marginal responsiveness or interest in responsible data stewardship.

In short, the socio-economic landscape forming the base case scenario for the socio-economic impact evaluations clearly demonstrates a misalignment between the existing and desired cloud computing landscape. However, this misalignment is no surprise as the A4Cloud project assumed stakeholders might not desire an accountable cloud computing landscape. Especially since the notion 'accountability' was a relatively new concept in the cloud market, transferred from the public sector to the private sector. The reason for this transfer, amongst others, is the information asymmetry between cloud providers and cloud customers / end-users. Introducing the notion of accountability in the market of cloud business models required cloud providers to change their behaviour with respect to their

[2] http://laws-lois.justice.gc.ca/eng/acts/P-8.6/
[3] http://www.bbc.co.uk/radio4/reith2002

customers. A4Cloud aimed for developing a combination of technical accountability tools, raising awareness and other 'softer' measures to achieve the desired behavioural change towards the envisioned accountable cloud computing landscape.

3.2 Identified mechanisms to steer accountable behaviour in the cloud

Whereas the first deliverable described the existing socio-economic landscape of cloud computing in relation to accountability, the second deliverable on the socio-economic context of accountability in the cloud (D24.2) focused on the stakeholders' behaviour and attitudes towards cloud and accountability and how they could be stimulated towards responsible stewardship through accountability. In this deliverable first incentives for promoting an accountable cloud ecosystem can be distilled.

Importantly, the various stakeholders demonstrated different perceptions on cloud computing and the way forward in promoting accountable behaviour in the cloud. Indeed, the socioeconomic landscape of cloud computing is, unsurprisingly, diverse and hence requires different types of tools and mechanisms to address the different types of cloud stakeholders. For example, individual end-users lacked awareness of potential risks related to using cloud services. Moreover, their uttered concerns with respect to the cloud did not match actual coping behaviour. Therefore, the effect of this mismatch between perception and practice (may) result in a lack of demand for accountability and accountability tools. The socio-economic research hence emphasized the need for raising awareness and sensitising the general public that there actually should be a need to promote and guaranteed the responsible handling of data in the cloud seems necessary. The organizational cloud customers inquired already demonstrated a clearer need for accountability of data stewards. For them the focus should lie in shaping the desired accountable behaviour via providing tools and governance mechanisms that fitted their needs. Proposed solutions for the A4Cloud project have been the stimulation of accountability from both a more societal and economic perspective. The societal perspective emphasized the stimulation of accountability in the cloud ecosystem via empowerment and engagement of end-users (so called cloud subjects). In order for cloud subjects to request for compliance to data protection and accountable behaviour by cloud providers and cloud customers, their first needs to be some transparency on what happens with one's data in the cloud. From an economic perspective emphasis was laid upon the need for compensating the asymmetric information relation between cloud providers and cloud customers. The economic model developed proposed the introduction of a private sector certification agency, comparable as to the current Cloud Security Alliance's role in the cloud. Simultaneously, the value of ethical accountability for cloud providers was demonstrated to be quite high. Acting in a responsible manner with entrusted data improved both the sustainability and health of the cloud ecosystem.

Both the input from the socio-economic landscape of cloud computing and the findings about how to stimulate accountable behaviour were presented to A4Cloud's tool developers. This allowed the tool developers to critically asses what cloud actor they should be targeting with their tool and how to target them best to warrant the greatest impact. Moreover, they also form the base-case scenario for the socio-economic impact analysis conducted and reported in this deliverable. We will study to what extent the developed accountability tools, though still in prototype, can have an impact on the cloud ecosystem in such way that responsible behaviour with data (entrusted with) in the cloud becomes not only a legal prerequisite but also the norm in cloud business.

4 Socio-economic impact analysis accountability in the cloud

The findings are presented in two parts. In the first part, we list the evaluations of each tool that was included in the study. In the second part, we highlight some key learning points of a general nature. These key findings are a combination of deductive analysis of the interview minutes and transcripts, secondary data analysis and statistical analysis of the online questionnaire. Our respondents have various backgrounds, and since some of them wanted to remain anonymous it is not possible to provide full details of every respondent. However, in the table below (Table 2) one can see the general descriptions of their roles, size of organization, and sector working in.

TABLE 2 Respondents' backgrounds

Respondent	Cloud role	Size organization	Sector
I	CSC	LE	Public
II	CSC	LE	Public
III	CSP / Cloud broker	SME	Public & private
IV	CSP	LE	Public
V	CSC	LE	Public
VI	Cloud customer	LE	Public
VII	CSP	SME	Public & private
VIII	Cloud broker	SME	Public & private
IX	CSP	LE	Private

4.1 Socio-economic impact by tool

We have asked the A4Cloud tool owners what they believed the development costs would be for bringing the prototype tools to production level and the adoption cost for the accountability tools.

TABLE 3 Development and adoption costs

Tool	Development cost	Adoption cost
DPIAT	6 person months	0
DPPT	25 person months	0
AAS	14 person months	0.25 person months
DT	9 person months	0.25 person months**
RRT	6 person months	
TL	24 person months	0.5 person months
IMT	18 person months	0.25 - 3 person months*

* depends on how much of IMTs capabilities are adopted

** provided that the company already knows which data is personal data and which data belongs to which user – if not, this number would increase significantly.

The estimated adoption costs are of relevance in comparison to the estimated costs by its potential users. While the respondents in both the interviews and the questionnaire did not attach any monetary value (either in euro's or in person months of estimated work) to the implementation costs as they deemed this to be quite difficult, their considerations with respect to costs are taken into account in both the descriptions below and in section 4.2 depicting the more general findings in relation to accountability in the cloud.

In addition we have asked questionnaire respondents to rate for each tool: the clarity of its description (good, fair or poor), and how much effort would likely be needed to implement the tools in the respondents' daily practice (great effort, somewhat effort, very little effort, no effort at all) (see Figures 2-8). Respondents were also asked to rate on a 5-point Likert scale (completely disagree – completely agree) the following four items for each of the accountability tools: a) The functionality of the prototype

tools would likely be useful in my daily practice, b) Using these accountability tools would likely improve the quality of the work I do, c) Compared to the tools I am currently using these tools seem more beneficial in demonstrating that I / my organization handles personal and/or sensitive data in a responsible manner and d) Using these tools will likely improve my organization's reputation as a responsible data steward (see Tables 4-10). The number of assessments per tool varies since we asked respondents to rate those tools relevant to them based upon their role in the cloud ecosystem as CSP, cloud customer and data subject respectively (see Table 1 in chapter 2). Of the 206 respondents 59 identified their main role in the cloud as data subject (28,6%), 137 as cloud customer (66,5%) and 10 as cloud service provider (4,9 %).

4.1.1 DPIAT

All CSC recognised the usefulness of DPIAT, but most were unsure if the tool would lead to significant cost reductions. DPIAT was seen as providing input into work that the IT-departments were already conducting, but the IT-managers we spoke to claimed to have sufficient awareness about the dangers of utilizing cloud services. As long at the output from DPIAT can't be regarded as legal advice, they felt that they could not rely too much on this tool. They would still need to undertake manual evaluation whenever considering to enter into business relations with a new service provider. One CSP referred to own experience, and survey results that he had seen, indicating that many CTOs and CEOs of large companies don't have a clear understanding about the risks and pitfalls of uploading data to the cloud. He thought that DPIAT had the potential to be very useful for improving others' understanding of how they should utilize the cloud.

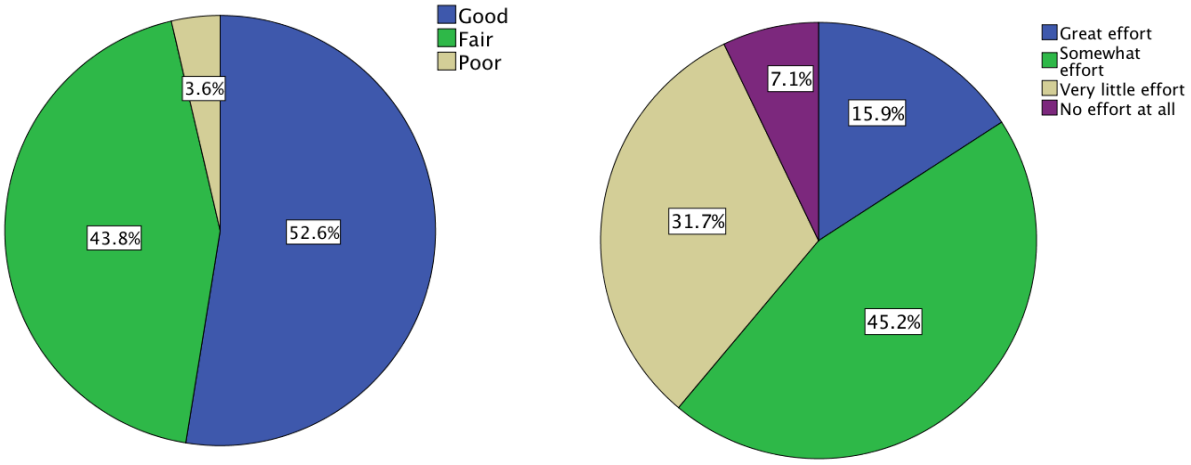

Figure 2 Clarity of the DPIAT description and effort expected for implementing the DPIAT tool

TABLE 4 DPIAT assessment

	N	Minimum	Maximum	Mean	Std. Deviation
DPIATfunctionality	127	1.00	5.00	3.6457	.86857
DPIATquality	128	1.00	5.00	3.6563	.82708
DPIATcomparison	125	1.00	5.00	3.6240	.86755
DPIATreputation	130	1.00	5.00	3.6462	.97933
Valid N (listwise)	117				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.2 AAS

Auditing CSPs is a daunting task for most cloud customers. In today's world, auditing requires hiring third party consultants, and this is seen as prohibitively expensive to be done on a case by case basis.

Instead, customers need to rely on annual auditing reports paid for by the CSPs themselves, based on standard data management policy. The prospect of an automatic and continuous auditing process based on custom policies was seen as attractive, since it would improve the frequency and relevancy of audits. There was general agreement that such a tool would be of "high value". One of the subjects mentioned that independent audits of their providers is something that he felt was part of his job, but something that he was unable to do presently. He did not see the tool as providing savings for the company, but it would definitively be regarded as increasing the quality of the service that his team provided to the organization.

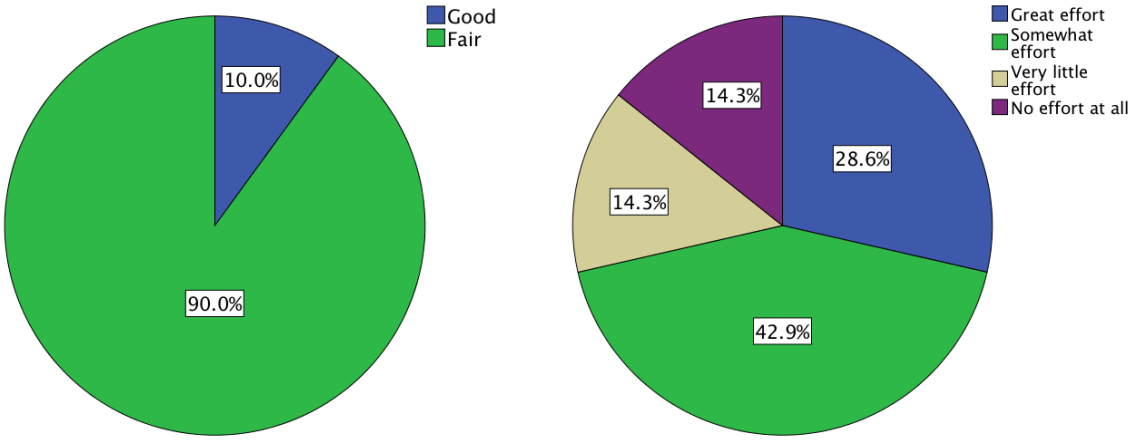

Figure 3 Clarity of the AAS description and effort expected for implementing AAS tool

TABLE 5 AAS tool assessment

	N	Minimum	Maximum	Mean	Std. Deviation
AASfunctionality	7	3.00	5.00	3.8571	.89974
AASquality	7	2.00	5.00	3.7143	1.11270
AAScomparison	8	2.00	5.00	3.7500	1.03510
AASreputation	7	2.00	5.00	3.7143	1.11270
Valid N (listwise)	6				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.3 DPPT

DPPT was seen as a system specific tool that was not immediately relevant to the customers. They could see how the tool would be useful for developing the set of tools that A4Cloud has developed. One broker thought that this tool was the most important of all the tools we presented, as it is the key to generating individualized policies at a large scale. It is generally very difficult to influence the data management policy of a large CSP, and the ability to set your own policy was thought to be of great value. The broker's impression was that data management policies of large CSPs are only differentiated at the country level. Some smaller CSPs already advertise data storage subscriptions that differ with respect to whether the uploaded data will be stored nationally, within EU or globally. This indicates that there is an existing demand for being able to influence how CSPs handle your data.

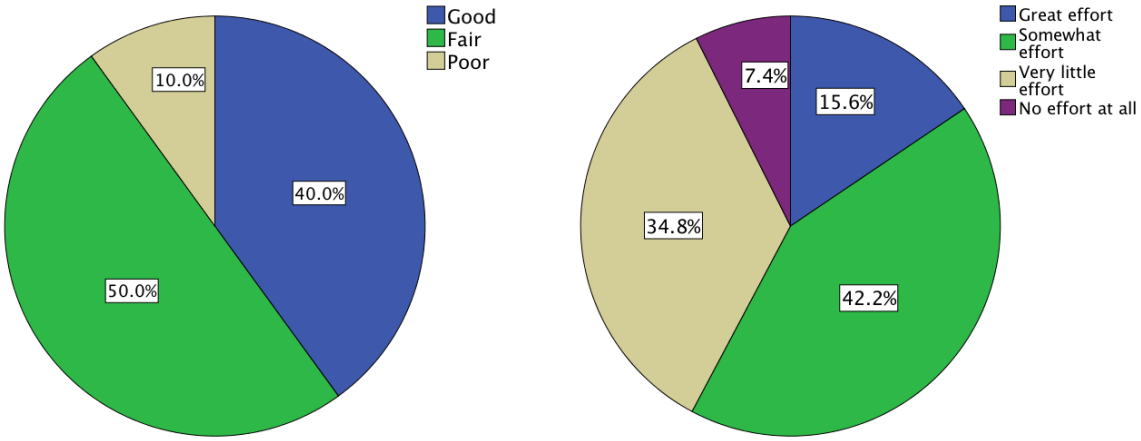

Figure 4 Clarity of the DPPT description and effort expected for implementing the DPPT tool

TABLE 6 DPPT assessment

	N	Minimum	Maximum	Mean	Std. Deviation
DPPTfunctionality	137	1.00	5.00	3.7810	.92128
DPPTquality	137	1.00	5.00	3.6934	.91203
DPPTcomparison	132	1.00	5.00	3.7045	.94698
DPPTreputation	140	1.00	5.00	3.7643	.94153
Valid N (listwise)	124				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.4 IMT

A tool for incidence management at the service provider was seen as a useful tool for preparing the businesses for stronger regulation, such as the GDPR. The relevancy of the tool is expected to rise as awareness about data stewardship increases. CSPs should find it useful to be able to argue that they have the necessary systems to comply with EU-regulation and their customer's needs. However, the customers that we talked to were not too concerned with exactly how the providers arranged their systems. Some subjects thought that tools with similar functionality already exist, and this raised a concern whether IMT would be cost-efficient enough to survive in the market. The main concern amongst the customers was whether they could rely on their contracted provider to truthfully disclose breaches and other incidences. A broker noticed that whenever one of their customers experienced problems with a service, then the broker could (and often did) send out warnings to other customers that were using the same service. However, the IMT tool would allow them to do this at a much larger scale, and was therefore of interest for them.

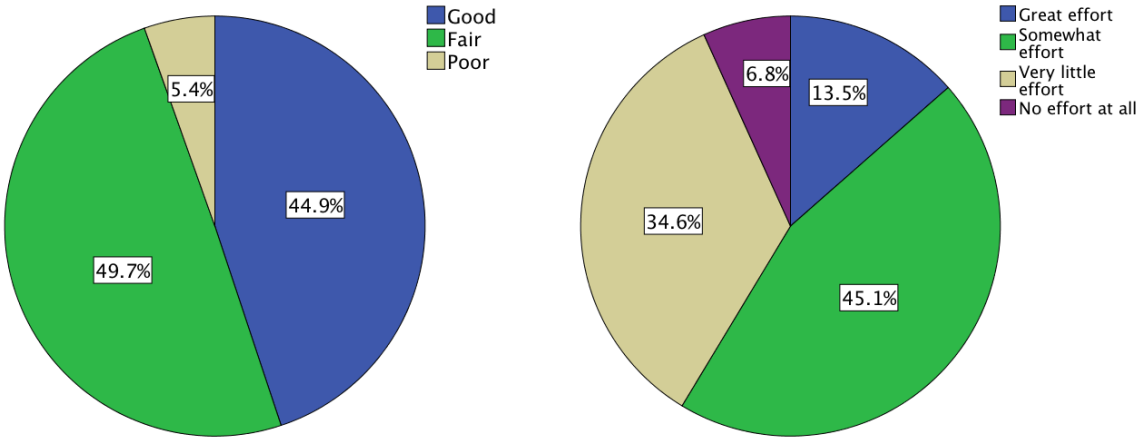

Figure 5 Clarity of the IMT description and effort expected for implementing the IMT tool

TABLE 7 IMT assessment

	N	Minimum	Maximum	Mean	Std. Deviation
IMTfunctionality	134	1.00	5.00	3.7090	.85686
IMTquality	139	1.00	5.00	3.6619	.86438
IMTcomparison	130	1.00	5.00	3.6000	.86804
IMTreputation	138	1.00	5.00	3.6957	.90100
Valid N (listwise)	121				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.5 RRT

A key comment regarding the RRT was that its usefulness depends on the number of incidences that need to be handled. As more and more data is moving to the cloud, the potential for negative incidences will continue to grow. In daily life, a relatively high proportion of the work of involves the more mundane and standardized task of dealing with lost and forgotten passwords. Data breaches are not yet seen as unmanageable. The overall evaluation of the tool was that it is somewhat ahead of itself and that it should be more useful in 5 years than it is today. One subject suggested that the tool should be endowed with the ability to learn from how users responded to incidences, so that the quality of RRT might improve over time.

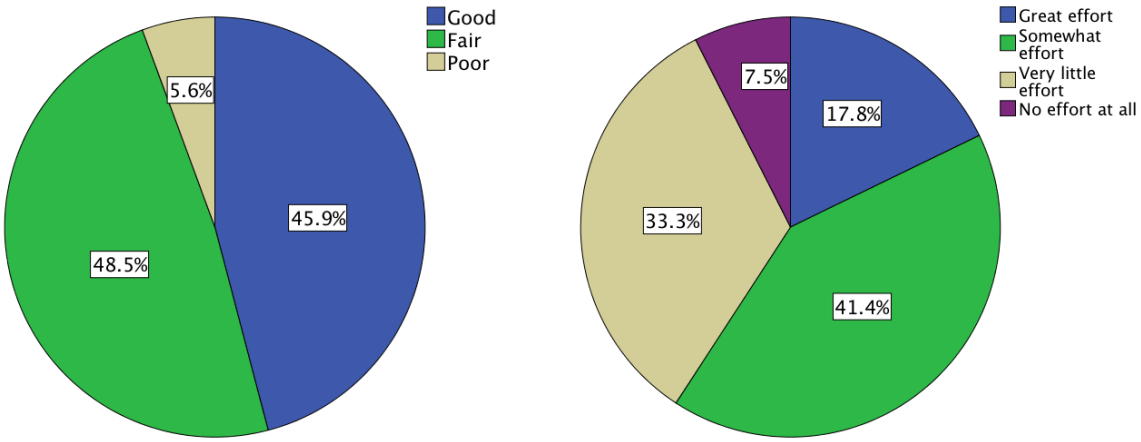

Figure 6 Clarity of the RRT description and effort expected for implementing the RRT tool

TABLE 8 RRT assessment

	N	Minimum	Maximum	Mean	Std. Deviation
RRTfunctionality	182	1.00	5.00	3.6593	.83725
RRTquality	185	1.00	5.00	3.5730	.88239
RRTcomparison	177	1.00	5.00	3.6271	.91512
RRTreputation	183	1.00	5.00	3.7158	.90549
Valid N (listwise)	166				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.6 DT

The DT tool generated considerable excitement. As almost every digital system has the potential to monitor and store large amounts of data, it is easy to lose track of what data is being disclosed to which provider. The customers were wondering more about what the providers are using the data for, rather than being concerned with sharing the data with the providers. As an example, they were more concerned with being able to define a policy for how localization information could be used by the apps and CSPs, rather than providing localization information. A lot of information is shared reluctantly under the presumption that it is necessary in order to use a service. One CSP questioned whether end users actually have any willingness to pay for protecting their privacy, as it seems that many people don't have a problem with compromising their privacy in return for free services such as Facebook. The broker said that it is easy to see how they could sell functionality such as the DT provides to customers, and that it should be attractive for CSPs to adapt to the tool. The customers were more concerned with whether it would be possible to make enough providers support the system so that it would become the tool-of-choice for allowing or denying providers access to personal data. It was seen as unlikely that customers would refuse to use a given service on the basis that is does not support DT. Some respondents also questioned the feasibility of the DT tool, especially with respect to the need for multiple stakeholders in the cloud chain to provide transparency about data whereabouts this was deemed unlikely.

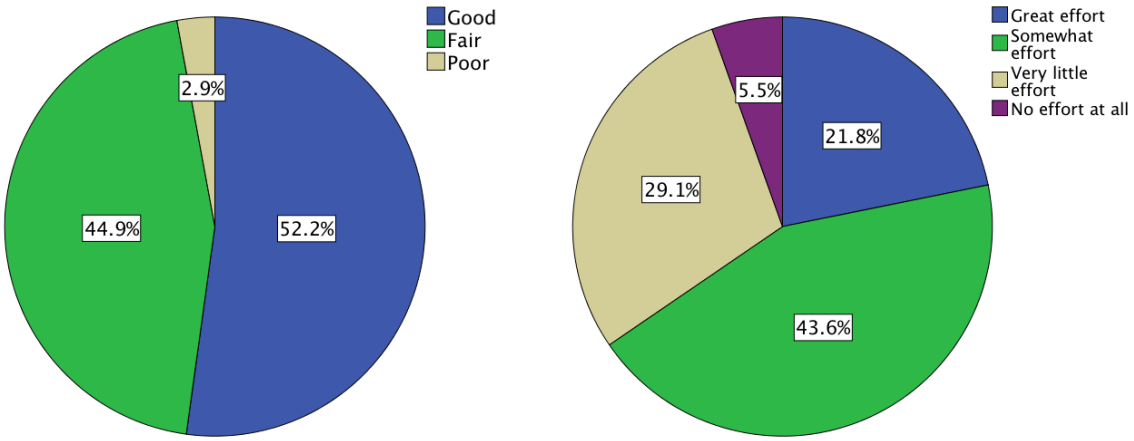

Figure 7 Clarity of the DT tool description and effort expected for implementing the DT tool

TABLE 9 DT tool assessment

	N	Minimum	Maximum	Mean	Std. Deviation
DTfunctionality	63	1.00	5.00	3.8254	.81398
DTquality	62	2.00	5.00	3.7097	.73300
DTcomparison	63	2.00	5.00	3.7619	.79746
DTreputation	61	2.00	5.00	3.8361	.84024
Valid N (listwise)	57				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.7 TL

The transparency log was considered of vital importance by some customers. If such a tool actually existed, it would be hard for large providers to argue why they were not using it. Not complying with such a tool would be seen as indicative that the provider had something to hide, and many customers would not wish to buy their services. Of all the tools that were discussed, this is the one that clearly was seen as having the potential to set a company apart from others if they could offer it.

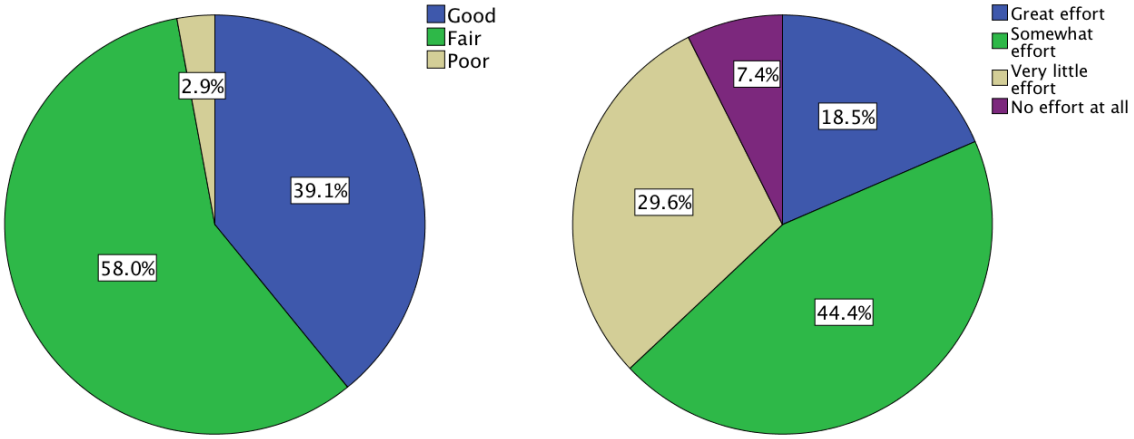

Figure 8 Clarity of the TL tool description and effort expected for implementing the TL tool

TABLE 10 TL tool assessment

	N	Minimum	Maximum	Mean	Std. Deviation
TLfunctionality	61	1.00	5.00	3.6885	.76466
TLquality	61	2.00	5.00	3.5902	.76107
TLcomparison	63	1.00	5.00	3.6032	.79392
TLreputation	62	2.00	5.00	3.6935	.80141
Valid N (listwise)	57				

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.1.8 General response towards A4Cloud's accountability tools

Most respondents indicated that, though they liked the idea of the prototype accountability tools, they deemed the description to be too scientific and hence too complicated to understand why one should need these tools. Another general finding is the feasibility of the tools. Both CSPs and cloud customers indicated that they liked the generic focussed feature of the tools, however questioned whether implementation was possible. Specifically because demands per type of organization

(public/private sector, type of data involved) differ so much, that the generic tools likely need quite some adoptions to fit the specific (IT) context.

4.2 Non-tool specific key findings

Below we describe the key findings of the SEIA that are not tool specific. The themes addressed here are based upon deductive analysis of the interview minutes and transcriptions and are complemented with findings from the online questionnaire. The thematic analyses of the interview minutes and transcripts are based upon the acceptance model developed in chapter 2 (see Figure 1). This means that the following information was abstracted from each minute/transcript: a) perceived usefulness of the accountability tools and its main features (including aspects as trust, quality), b) perceived risks or costs related to adoption of accountability tools, c) internal organizational characteristics and d) external organizational characteristics influencing accountability tool adoption. By reading an deductively coding the minutes/transcripts we could determine key concepts, themes and patterns relevant for understanding the likely adoption of accountability tools. The questionnaire results depict the responses of a more general type of cloud customer than the interview respondents. As a consequence the questionnaire can provide some indication for how the accountability tools and specifically the main values of accountability are valued by a larger audience.

4.2.1 (Social) costs of accountability in the cloud

The tools are unlikely to lead to significant cost reductions for the cloud customers. While some tools, such as DPIAT, has the potential to improve IT-managers efficiency when considering entering into agreement with a new CSP, it is seen as unlikely that the tools will free up sufficient time to do other tasks. Instead, the tools should be regarded as an additional option that IT-managers have when conducting their work. In some cases, the increased quality that the tools provide will make companies pay more attention to, and spend more (not less) resources on, data management.

Moreover, interview respondents indicate that work is needed to implement accountability, not only the tools but also the entire ‘code of ethics’ that is behind this process. If businesses want to adhere to this accountability notion of being able to comply with data protection regulation and to demonstrate such compliance at any given time in point, this means that cloud service providers and SMEs using these services need to rebuild and restructure their architecture and IT infrastructure. In other words, introducing accountability in the cloud often also entails introducing accountability in non-cloud environments since most of the CSPs and cloud customers we interviewed indicated that many cloud customers still have hybrid environments (both cloud and non-cloud IT infrastructures). Hence, it is of importance that cloud stakeholders are able to choose the accountability tools and mechanisms that best met the context and environment of their organisation.

Exactly the required work compared to expected RoI seems to indicate that costs, as in required effort, might be deemed too high (see also Figure 9). For example, respondents who tried to build in more control for patients over their data or provide criteria for assessing stakeholders in the cloud chain noticed a low interest in their services by their potential customers. As one CSP respondent indicated: “for a while now we try to put patients more in control of their own care process [and thus also their data]” […] “however, this is quite difficult as these patients do not pay our bills”. (respondent IV).

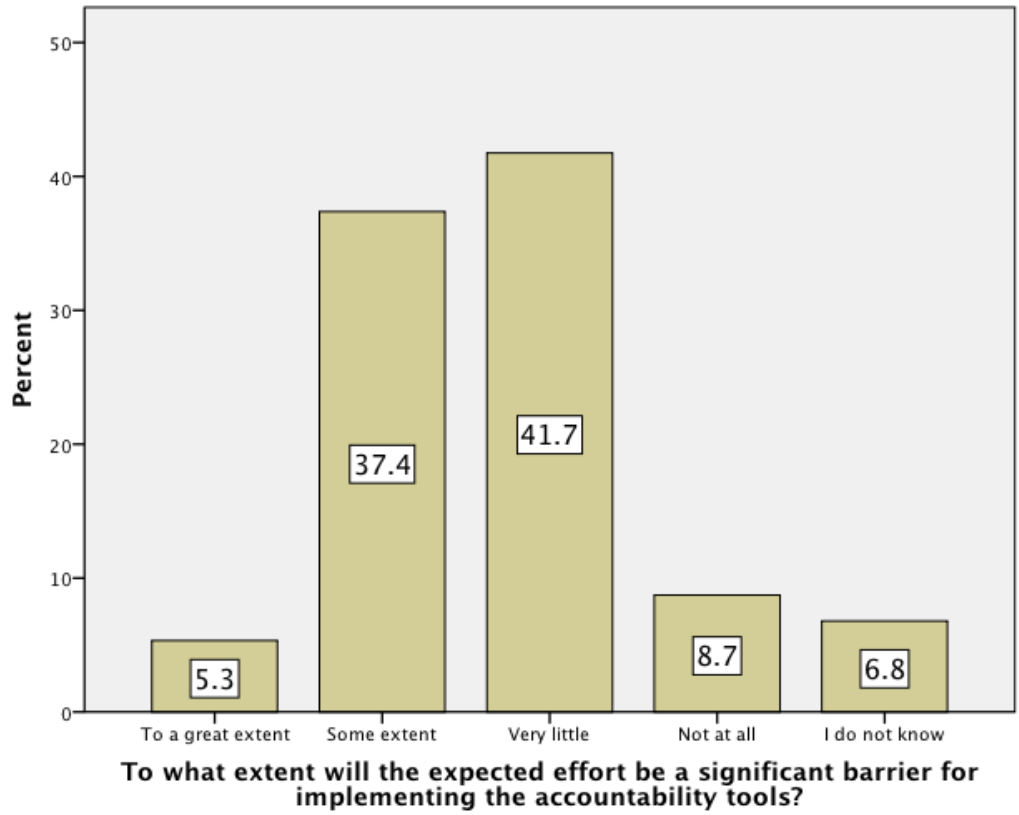

Figure 9 Effort as barrier for implementing accountability tools (N=206)

Organizational restructuring

The required organizational restructuring for adopting responsible data stewardship in once organization largely depends on the existing business culture within a company. If the current code of ethics within the company already emphasizes the need for warranting privacy and data protection, the required organizational restructuring is expected to be quite small in effort. However, changing the direction of existing business culture requires a longer breath. The CSPs that already felt the need to embrace responsible data stewardship indicated they were already conducting various certification processes, there company entailed one or more data protection officers in order to demonstrate their business culture was ingrained with a general respect for personal data. “However, this business culture requires not only to have the organizational process described well [as in certification processes], but also to act according to the principles of responsible data stewardship” (respondent IV). The latter is often more difficult to establish since this also requires some physical components to fit the non-physical requirements for upholding accountability in the cloud.

IT architecture restructuring

Lack of integrated systems, fragmentation of third-party applications for population health management hamper many accountable care organizations. So, if businesses want to adhere to this accountability notion of being able to comply to data protection regulation and to demonstrate such compliance at any given time in point, this mainly means that CSPs and SMEs using these services need to rebuild and restructure their architecture and IT infrastructure. Importantly, one respondent claimed, accountability should not be an afterthought. Accountability, security and data protection should be elements ingrained inside of the design thinking of the IT systems (respondent VII). The same respondent who indicated that the organisational restructuring was not that bad to do since the company already embedded the culture of respecting data indicated that the technical steps necessary to make a cloud solution compatible to the new GDPR requires an awful lot of work. The company started working on developing data protection compliant tools and solutions two years ago and expects that three more years are necessary to finalize the IT architecture restructuring of the company (respondent IV).

Perceived risks

None of the interview respondents indicated any risks attached to including accountability in the cloud. The security threat analysis performed in the next chapter (see chapter 5), seems to confirm this. The only risks mentioned that might be of relevance are the risks of not complying to data protection regulation and reputation damage (see section 4.2.3).

4.2.2 (Social) benefits of accountability in the cloud

On the one hand, the accountability tools may lower entrance barriers for new cloud service providers. Cloud computing relies, to a large extent, on economies of scale. Data storage, processing power and marketing is all cheaper per unit the bigger the company is. This makes it hard for new companies to compete with existing ones. One CSP thought that the accountability tools may offer some advantage to smaller companies in that they may be able to offer greater flexibility in data management than the biggest companies are willing to. Also, new companies are generally seen as less trustworthy than those that have been in the market for years. Therefore, new companies have more to gain from signalling trustworthiness through the use of tools such as the AAS and IMT.

On the other hand, the accountability tools also aim for decreasing the information asymmetry between CSPs, cloud customers and data subjects. However for some of the CSPS, specifically those offering (almost) free services in exchange for data, their underlying motives seem to be quite unclear. According to our respondents, CSPs are not likely to easily provide their underlying motives or business models. Respondents thus expect that A4cloud tools that provide increased transparency about data whereabouts (e.g. Data Track) and underlying business models might level the playing field between CSPs and their customers a bit.

Perceived usefulness

Current descriptions of A4Cloud accountability tools in general are rated by the expert respondents as fair or quite clear, likewise the questionnaire respondents (see Figures 2-8). However, they are also perceived as targeting a research audience and not a business audience. From the descriptions it does not become clear why a software vendor would be interested in these accountability tools as they insufficiently show what problem the tools address. Since accountability remains a rather vague notion to most cloud vendors and cloud customers, these problems should be more tangible or make explicit reference to the upcoming changes in the legal framework for data protection regulation within the EU (respondent VII).

The A4Cloud tools are of interest to CSPs as they offer scientifically based instruments that offer guidance in compliance to data protection and simultaneously does not require CSPs to develop these tools themselves, hence saving valuable business time. However respondent VII indicates, his company would definitely be interested in the AAS and also in the DPPT. Especially the AAS is not an easy system to build. In other words, being able to demonstrate compliance is not easy though desirable.

Preconditions for accepting the A4Cloud accountability tools refers to the ease of implementation. While ease of implementation and use are deemed important, current tool descriptions do not explain much about how such implementation is envisioned (respondent VII). This concern is shared by other respondents, especially since sectors are so different (example provided was healthcare compared to energy sector) it was questioned whether the generic tools would offer the necessary user-interfaces for each of these sectors.

Nevertheless, the main features of the A4Cloud accountability tools are expected to help out in demonstrating accountability in the near future. *"They seem to enable me to demonstrate various components required from law" (respondent VII).* Moreover, the tools and mechanisms tied to the accountability tools seem to fill in the gap in standardized decision-making procedures that has emerged since the 'cloudification' (the conversion and/or migration of data and application programs in order to make use of cloud computing) of the IT-sector. Whereas, in the pre-cloud area most companies had IT-departments responsible for careful decision-making in IT-adoption, the cloudification has resulted in more fragmented decision-making due to the ease with which companies can get acquainted with cloud services. Increasingly CEOs or heads of departments introduce new cloud services they have got themselves familiarized with at home or via their networks into their company without proper consulting of the IT-department (respondent III). "Especially since these IT-departments were a perceived synonym for the 'no-culture', in which many desired functionalities were

not possible" (respondent III). The accountability tools re-introduce guidance on proper decision-making via, for example Cloud Offering Advisory Tool (COAT) and DPIAT tools, and offer standardization of auditing processes of cloud services or conditions against which the use of certain cloud services can be tested. Exactly this aspect of the accountability tools is deemed useful by some of the respondents.

Perceived quality

The tools may lead to significant quality improvement for cloud customers. They are seen as providing cloud customers more insight in, and influence on, how data is managed in the cloud. They are also seen as mechanisms for making the cloud providers more responsive to the needs of their customers. The possibility to tailor data management policies to a specific project, or a class of data, is likely to increase the use of cloud services. The tools will thus improve data management on the customers' side as well, and IT-departments will be able to provide better quality-of-service for their end users.

Reputation

New EU-legislation, specifically the GDPR, will probably boost demand for the accountability tools. With the GDPR, the potential fees for mismanaging privacy data will rise. The new legislation is also likely to increase public awareness about data privacy. This makes it more likely that unfavourable coverage by mass media will significantly hurt a company's reputation. Both mechanisms make it more important for companies and organizations to be able to argue that they do what they can to protect their data. One way to do this could be to engage in more business with CSPs that offer one or more of the accountability tools developed by A4cloud.

Companies that already develop their IT architecture in such way it supports and entails data protection requirements often expect a RoI on incorporating accountability in their organisation and IT architecture. More specifically, they anticipate that as quality instruments in the past, accountability will become an important notion in the near future market. Being able to demonstrate one's responsible data stewardship becomes part of having a good reputation, hence increased trust by potential customers.

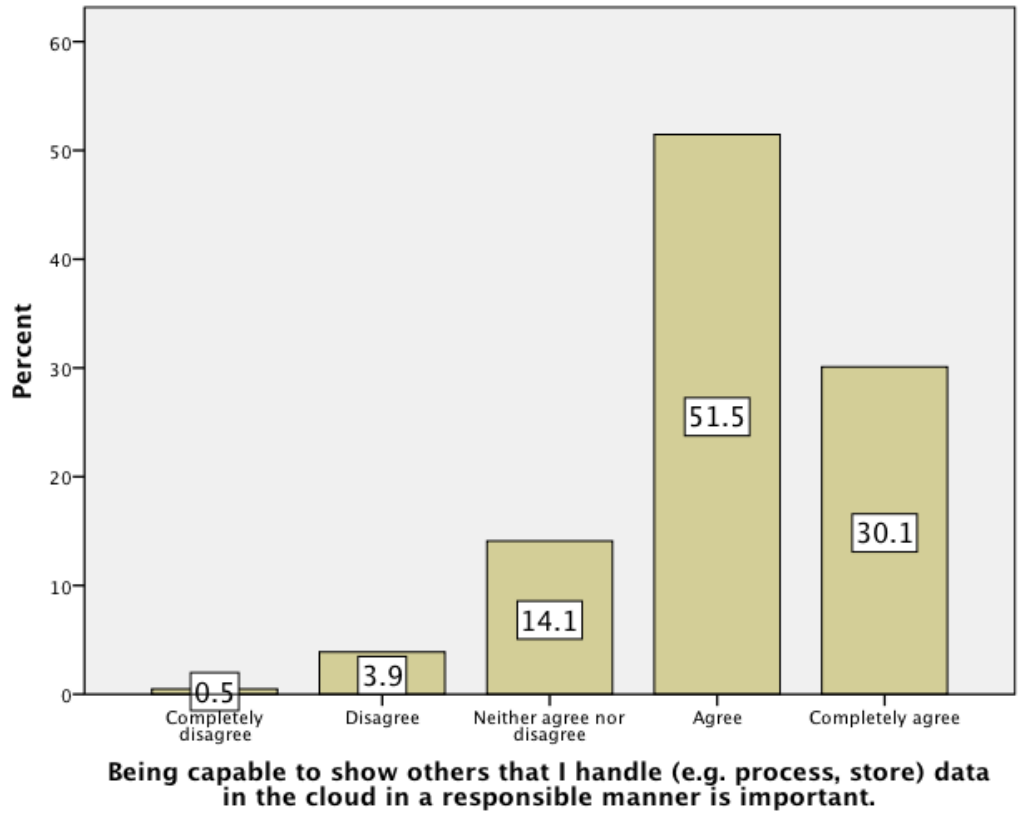

Figure 10 Importance of being able to demonstrate responsible data handling

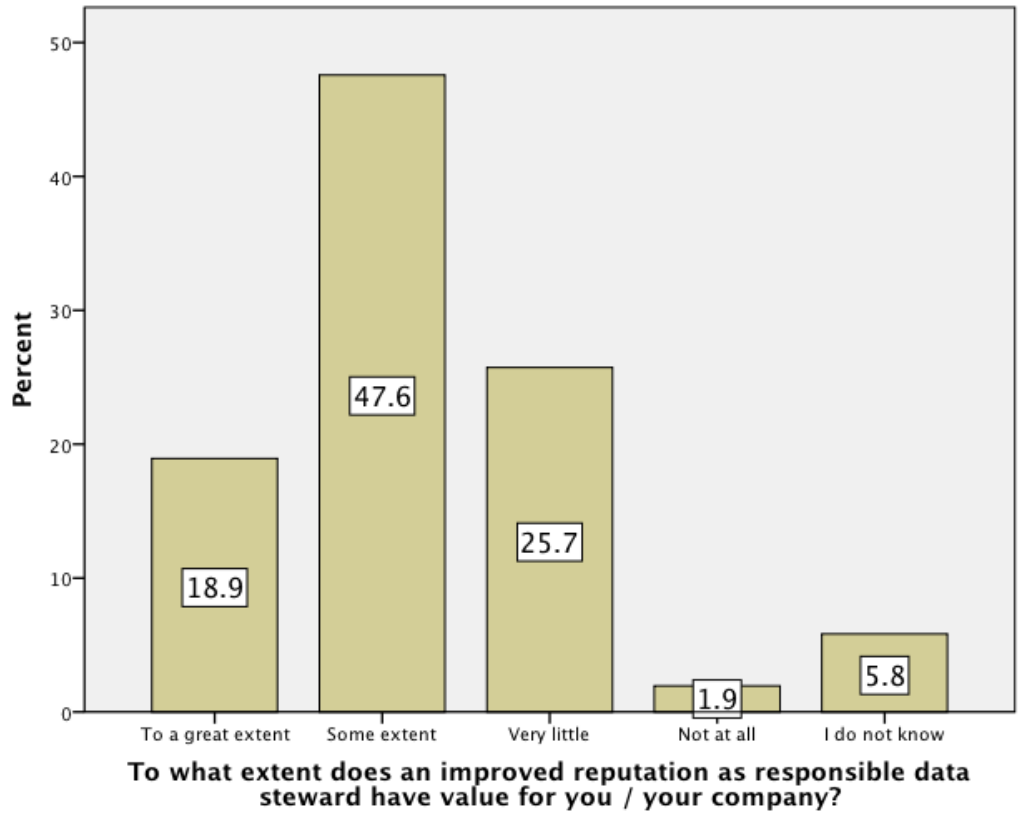

Figure 11 Value of improved reputation as responsible data steward (N=206)

Remarkably, the respondents in the interviews indicate a different attitude to being able to demonstrate responsible data handling than the questionnaire respondents (see Figure 10). Importantly, the interview respondents indicate that responsible handling of data for other than business purposes, i.e. from a more societal perspective, is not necessarily a main driver for SMEs. Apparently, the respondents from smaller business regard this as a rather philosophical aspect, i.e. something you develop from a personal perspective on how to properly handle data in the cloud and not something that ties into reputation, business models and good governance of data in the cloud. While the questionnaire respondents indicate that being able to demonstrate responsible data handling is important (M.= 4.07, S.D. = .800, N = 206), the value of responsible data stewardship for the reputation of a company is rated somewhat lower (M.=2.28, S.D.=.987, N=206) (also compare Figure 10 and 11).

Larger corporations often deem reputation as a responsible steward also important from a more ethical stance towards accountability. A good reputation as a large company is part of the business model (respondent IV). In that sense, increasing awareness by offering information on what happens with data, as the data track tool for example does, is considered one of the top priorities stimulators of data stewardship should have. Importantly, the A4Cloud's accountability framework and tools aim to go a step further than corporate social responsibility has done in the past.

4.2.3 General attitude towards accountability in the cloud

Since accountability has many different meanings, and means different things for different stakeholders, a simple cost-benefit analysis is not possible. For some it entails procedural workflows according to legal requirements. Others perceive it as others taking care of all necessary security mechanisms to warrant responsible data handling. Thirdly there are some businesses that perceive accountability as important from a business perspective. Last, there are businesses deeming accountability of importance not only because of legal requirements or business value, but also because responsible data stewardship is the right way to handle data in the cloud (respondent VII). The last category resembles the A4Cloud approach to accountability best. Respondents focussing on

these type of accountability relations between cloud stakeholders aim for engaging in cloud relations based upon careful decision-making, taking into account responsible data handling, and the consequences of this relation for both continuity within the organisation and dependency of cloud customers towards the CSP.

The complexity of the accountability notion also increases the difficulty in making balanced or well-founded analysis whether to adopt or not adopt more responsible behaviour towards data in the cloud. According to some interview respondents, accountability involves a change of perception on the relevance of data and the jurisdiction of data. Moreover, if businesses want to adhere to this accountability notion of being able to comply to data protection regulation and to demonstrate such compliance at any given time in point, this mainly means that CSPs and SMEs using these services need to rebuild and restructure their architecture and IT infrastructure. The business model for accountability thus requires not perceiving accountability as something enforced by regulation, but as something one should invest in for having long-term revenues.

However, smaller CSPs indicate that the need for security and data protection as perceived by their customers is rather low. First, because for some of their customers, cloud computing is still something difficult to grasp. Regularly, people think that their data is physically still present in their own IT environment, on their own devices, states respondent III. Clear mental models of what happens to their data in the cloud is difficult. As a consequence, cloud customers often have a rather reactive and not proactive approach to security and data protection. Second, because in current business models the functionality of cloud services are deemed of more importance than accountability (respondent III). It is this poor trade-off, the economics of cloud computing that plays an important role in the general hesitance of CSPs and cloud customers in accepting accountability tools and mechanisms in the cloud system. Where's the profitable business in responsible data stewardship?

The general attitude towards accountability and data protection in cloud ecosystems thus often is indicated to be quite polarized: there is a large group of people who do not believe that actual enforcement of the GDPR will happen, especially since large parts of society (i.e. the lay general public) do not seem to care much about privacy anyway. On the other side there are these strong protectors of data protection and privacy for whom the GDPR is not perceived as severe enough. However, a respondent claims: "for these privacy fanatics the measurements will never be severe enough" (respondent IV).

Importantly, cloud customers indicate they are prepared to adopt a number of the accountability tools, if they are made available by CSPs. The demand for responsible data stewardship cannot be judged on the basis of observed behaviour alone. In many cases, customers feel that they do not have an actual choice in deciding how much data to disclose, even if they disagree with, or simply don't know, how the provider plan to use their data. The quality of the service they receive is seen as sufficiently good to make it worth compromising on privacy. It is also hard to separate those who refuse to use a service based on it data policy from those who are simply not interested in that service. Every customer that we have spoken to has been interested in improving their control over how their data is managed in the cloud.

The questionnaire results demonstrate how cloud stakeholders rate the importance of key characteristics of accountable behaviour in the cloud. The 12 items in this scale have a Cronbach's α of .859, p<.000, additional factor analysis demonstrated that the three willingness to pay items can be regarded as a subscale (items I, J & K). Importantly, despite the relatively high value addressed to compliance (items A, C & G), the actual willingness to pay for accountability is rated considerably lower (items I, J & K). The rather positive attitude towards accountability and its main features depicted in the questionnaire is not necessarily reflected in the more nuanced perspectives given by the interviewed respondents. The difference in these perspectives might be explained by potential recording of desired behaviour (questionnaire respondents) on the one hand and actual experienced behaviour (interview respondents) on the other.

TABLE 11 Perceptions on main accountability features

	Please indicate your perception on the following statements.	N	Mean	S.D.
A	Cloud service providers should be able to demonstrate how they comply with data protection regulation at any given moment upon request	198	4.20	.810
B	Transparency about specification and implementation of accountability	193	4.03	.832

	policies adds value to the business process			
C	Cloud customers should be able to demonstrate how they comply with data protection regulation at any given moment upon request	196	4.03	.768
D	Information on how cloud service providers protect data influences my decision to go into business with them	198	4.01	.793
E	When a cloud service provider gives increased control over the way personal/sensitive data is handled in the cloud this encourages my usage of its services	194	4.01	.785
F	Cloud providers must offer negotiation of who may do what with customers' data (e.g. via service level agreements)	193	3.96	.724
G	Damage due to data protection incidents should be remediated	199	3.88	.928
H	Information on how cloud service providers may use my personal / sensitive data allows for better choices in the selection of cloud service providers	198	3.87	.830
I	I would pay for services that offer insight in who has access to my (organization's) personal / sensitive data	195	3.70	.938
J	I would pay for services that offer insight in how I am doing with respect to protecting data I am entrusted with	190	3.68	.913
K	I would pay for services that offer control over how I am protecting data I am entrusted with	191	3.65	.932
L	I only work with (other) cloud service providers I have worked with before	194	3.44	1.002

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

4.2.4 Organizational and sector characteristics for accountability acceptance

Organizational characteristics (internal / external)

Based upon the interviews we aimed to find out whether organizational characteristics can be indicated to shape the likelihood of acceptance of accountability in the cloud ecosystem. In addition, the questionnaire gave insight in what organizational characteristics might be decisive in future acceptance of accountability tools and the awareness of current trends and requirements with respect to data protection. The 11 items in this scale have a Cronbach's α of .874, p<.000, additional factor analysis demonstrated that the external organizational characteristics can be regarded as a subscale (items B, D, E, G, & I).

Internal organizational characteristics refer, for example, to the size and type of the organization, management attitudes toward a technology or aspect thereof, degree of concentration for decision-making within the organization, level of bureaucracy and degree of openness (see items B, D, E, G, I in Table 11). Apparently, the CSPs interviewed had an intrinsic interest in the topic of accountability in the cloud. One respondent even indicated that the reason to participate in the interview was because of his interest in the A4Cloud project (respondent IV). Importantly, all CSPs indicated that their organization's awareness of the need for accountability was quite high. A respondent from a larger CSP (with 11 different departments and in total approximately 800 employees in total) indicated because his department was oriented towards the public sector and specifically the health care market, they were the leading department in developing new tools and policies in line with the new GDPR, but more importantly in line with their own privacy respecting culture. They shared their findings, tools and policies with the other departments to increase awareness for data protection and privacy across the entire company. Moreover, despite the fragmentation in different departments, it was recognized that if one of the departments failed in protecting a client's data, this affected the reputation of the entire company. Moreover, research by Tableau shows that larger companies often had CISO's and hence data protection was higher on the agenda while smaller companies had less resources left to spend on data stewardship [41].

External organizational characteristics are about the greater socio-economic context in which the organization is situated and refer to e.g. legislative pressure, sector-specific norms (e.g. regarding

data protection) and relationships with other public or private organizations (see items F, H, J, K in Table 11). The interviews demonstrated that organisations' willingness to adopt accountability was highly influenced by the expected new GDPR. The active enforcement of the GDPR is a prerequisite for creating data protection awareness by CSPs, cloud customers and potentially even cloud subjects. Cloud customers claimed that often their customers would feel restricted in the usability of the offered tools (respondent IV).

Moreover, a comparable example has been the recent enactment of the Bill on notification of data leaks.

> The law imposes an obligation on "data controllers" (the persons or entities that determine the purpose of and means for processing personal data) in the Netherlands to notify the Dutch Data Protection Authority (CBP) and affected individuals. The law may require data controllers to update agreements with their data processor to account for breach notice obligations. The law also increases fines for violations of the Dutch Data Protection Act (DPA) to up to €810,000 or 10% of the company's net annual turnover. Both data controllers and data processors (who may be deemed "accomplices" in the breach) may be subject to the fines[4].

While Dutch respondents agree that the Bill was carefully constructed, its enforcement is less likely since the CBP lacks the resources (financially and in personnel) to actively pursue reported data leaks. One respondent estimated this would be a merely 0,5-0,1% of the reported cases. If a similar situation would occur with the new GDPR, then despite all efforts this would have a low impact on the cloud ecosystem. Also, given the expected enactment in April 2016 and its 2-year implementation period, active enforcement would entail setting an example of several companies at 'Day 1' after completion of the implementation phase. Most respondents confirmed that the acceptance of accountability in the cloud ecosystem seems to highly depend on the enforcement of the GDPR in the near future.

Last, some CSPs indicated that their customers' level of knowledge with respect to the complex architecture of cloud computing and the specialized knowledge required for understanding the data protection requirements is not always adequate enough to give an appropriate interpretation of what necessary technological and organizational measures should be taken to support accountable data handling.

TABLE 12 Organizational characteristics

	Please indicate for the organization you represent your perception on the following statements	N	Mean	S.D.
A	Data protection is important	197	4.47	.812
B	Following existing practices, policies and protocols related to data protection and privacy is the norm	190	4.18	.783
C	My organization already makes use of mechanisms and tools demonstrating it handles data in the cloud in a responsible manner	188	4.16	.794
D	My organization consists of members/departments each having their own specialized knowledge and expertise	187	4.12	.884
E	The (top) management is likely to accept changes that accompany IT innovation	185	4.09	.836
F	The increased societal interest in data protection and privacy has changed my company's attitude towards handling data in the cloud	181	4.04	.852
G	Security of data residing in the cloud is an executive / board-level concern	183	4.04	.951
H	My organization has close ties with auditing or advisory institutes regarding data protection	184	3.90	.995
I	My organization has a strong hierarchical structure	187	3.88	1.043
J	The upcoming data protection legislation requires my company to make	174	3.86	1.016

[4] See: Norton Rose Fulbright Data Protection Report, http://www.dataprotectionreport.com/2015/06/breach-notice-becomes-law-in-the-netherlands-11-things-to-know/

	changes in its IT infrastructure			
K	The upcoming data protection legislation requires my company to make changes in its organization	176	3.79	.989

5-point Likert scale: 1: completely disagree, 2: disagree, 3: neither agree nor disagree, 4: agree, 5: completely agree

Sector segmentation

Based upon the interviews we could identify two types of segmentation: a) a segmentation based upon the size and maturity of companies and b) segmentation between the public and private sector.

Size of cloud customers companies matters. Customers see little scope for influencing large CSPs unilaterally. Large CSPs do not have much willingness to respond to single customer's demand for a tailored privacy agreement. One of our subjects had tried asking Microsoft and Google to change their policy as part of a large public acquisition, but neither agreed. There was broad agreement among the interview subjects that only national, or super national, governments have sufficient influence, through laws and regulation, to make large companies respond to customer demand for privacy. Larger enterprises or a partnership of several (larger) organizations within a specific sector do seem to provide room for negotiation between CSPs and cloud customers. For example, "SURF is the collaborative ICT organisation for Dutch higher education and research. SURF offers students, lecturers and scientists in the Netherlands access to the best possible internet and ICT facilities" [5].

Within the SMEs a distinction can be made between digital natives, modern start-ups, and to non-digital natives. The former seem more suited to cope with IT-architecture restructuring. The accountability tools and mechanisms developed by A4Cloud likely have an easier fit within these organizations. However, these start-ups like other SMEs seem to have little resources for focusing on data protection requirements. SMEs are expected to particularly focus on the favourable business model, in which functionality outweighs accountability.

Segmentation between public and private sector The public sector is likely to have more interest in the accountability tools and framework as promoted by the A4Cloud project. This increased interest can be explained by existing 'good governance' structures in the public sector as well as the need for demonstrating accountability already present [42]–[44]. Several respondents that had experience in the public sector referred to the healthcare domain as one of the most complex domains with high need for accountability. *"We do have had quite a few interviews with customers on accountability. [ok] because one of our market is the healthcare market. So there are lots of legal requirements and the need for specific certification and accountability is one of the most important areas there" (respondent VII).* Moreover, the public sector is also deemed to be a role model; either because they handle sensitive information, or because they are more visible to the public eye (respondent III, respondent IV). Nevertheless, to the surprise of our respondents, it is often the public sector that lacks careful decision-making with respect to cloud relations they engage in.

Interestingly, the financial sector, though private also was mentioned several times as a sector demonstrating interest in accountability. Explanations provided for this interest pointed at the recent crises in the financial sector and the increased control by government or governmental bodies. Parallels can be drawn between the financial sector and the cloud computing sector with respect to composite products offered. These composite or bundled financial products require high-level understanding to grasp what they do and only a few customers actually have that understanding. In comparison, the cloud ecosystem is offering similar composite products offered via opaque cloud chains that only a few people truly understand. Whereas the financial sector had a supervisory body, this is lacking in the case of the cloud ecosystem*"* (respondent III).

However, in contrast, interviews with institutional cloud customers demonstrated they rely heavily on government advice, policy and regulation when defining their own cloud computing policies. Both public institutions and private companies, such as global banks, rely primarily on formal regulation when deciding their data management policies. Neither wants to spend more money on data security than they are required to by law. Also, all though they may be uneasy of storing data in a foreign jurisdiction, saying so is seen as politically sensitive. Without a government advice against storing sensitive data in a given country, such as China or Russia, large institutions usually will not discriminate CSP based on nationality.

[5] https://www.surf.nl/en/about-surf

4.3 Summary

In general, most respondents expressed great interest in the A4cloud project. They were able to see how the tools would be helpful for their own organizations, and how the tools would add value for both cloud customers and cloud service providers. As expected, the participants differed somewhat in which tool they thought was most valuable. This difference can be attributed to the role that the subject had in the cloud service value chain. There was also general agreement as to whether the tools will replace already existing provisions to ensure accountability on the side of cloud service providers, and whether access to the tools can lead to a significant increase in data security and service quality.

The main point of disagreement that we encountered concerned the timing of the project with respect to the market's willingness to pay for increased accountability. Representatives at a company that classified itself as a cloud service broker, thought that the market may yet be ready to pay for tools that focus on tasks which cloud customers do not yet undertake, for example the AAS tool. The cloud customers that we talked to, on the other hand, expressed an interest in the accountability tools because they would enable them to conduct tasks which they otherwise were unable to take on.

General agreement exists with respect to the need for active enforcement of the new GDPR in order to warrant the introduction of accountability in the cloud ecosystem. Cloud customers confirmed CSPs opinion that without enforcement customers would prefer functionality over accountability features and hence have a very low willingness to pay for accountability.

5 Security Threat Analysis

An important aspect that helps to the SEIA is to understand the new risks that might arise as a consequence of the adoption of the A4Cloud tools. In the following, we will identity these security risks and assess their impact.

5.1 Methodology for Security Threat Analysis

In order to perform a consistent analysis of the security threats of the selected tools, it is necessary to follow a methodology that provides a structured and well-defined approach. There are several widely-known methodologies for security threat analysis, such as those provided by OWASP, CORAS, Microsoft, etc. [45]–[47]. In this section, we will follow the OWASP Application Threat Modelling methodology. According to this methodology, for each analysed tool, it is necessary to produce a different threat model, which will contain the necessary information for identifying and analysing threats. The steps that we need to follow are the following:

1. To document the most basic information regarding the tool:
   - Tool Threat Model Identifier
   - Tool Name
   - Description
2. To identify the external dependencies of each tool. The external dependencies are important since they may represent a threat (or be part of a threat) to the analysed tools, which is out of the control of the tool developer. For each tool threat model, it is necessary to provide the following information regarding external dependencies:
   - Dependency ID
   - Dependency Name
   - Dependency Description
3. To identify the entry points and interfaces accessible by each tool. These points are critical, since they are necessary for most attacks. For each entry point, it is necessary to provide the following information:
   - Entry Point ID
   - Entry Point Name
   - Entry Point Description
4. To identify of the assets that represent threat targets (e.g., users' data, credentials, policy repositories, etc.). The following information should be provided:
   - Asset ID
   - Asset Name
   - Asset Description
5. To describe the trust levels, which represent the different access rights that are used within each tool. Trust levels are directly related to entry points and assets, which helps to analyze their access rights. It is necessary to provide the following information:
   - Trust Level ID
   - Trust Level Name
   - Trust Level Description

Once that the initial information for each tool is collected and documented in the threat model, we can continue with the actual identification of security threats. In order to follow a systematic and structured process, we will try to elicit threats according to a predetermined threat categorization called STRIDE [47]. According to this categorization, threats can be classified according to 6 possible attacker goals:

- Spoofing: This type of attack consists in using another user's authentication credentials (e.g., user/password, private keys, etc.).
- Tampering: The attacker performs malicious modification of data, such as unauthorized changes made to persistent information and the alteration of communication data.

- Repudiation: The attacker may deny performing some actions, without other parties having any way to prove otherwise.
- Information disclosure: The attack exposes information to entities who are not supposed to have access to it.
- Denial of service: This type of attack implies the obstruction or denial of certain service to valid users.
- Elevation of privilege. An attacker gains privileged access to the system, and can potentially compromise or damage the entire system.

For each tool, we will identify risks associated to each category, taking into consideration the dependencies, entry points, assets and trust levels described in the threat model. For each threat that is extracted, it is necessary to identity the following information:

- Threat ID
- Threat Description
- Threat Category (STRIDE)
- Vulnerable point

The next phase of the threat analysis is the assessment of the risks associated to the threats. According to NIST Guide for Conducting Risk Assessments [48], "*risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of: (i) the adverse **impacts** that would arise if the circumstance or event occurs; and (ii) the **likelihood** of occurrence*". The likelihood or probability of occurrence is defined by the ease of exploitation of the threat, while the impact depends on the extent of the potential damage. We will follow these definitions of risk, likelihood and impact, which will serve as a basis for estimating the risk of each analysed threat.

Specifically, we will identify three different levels of likelihood and impact. With regard to likelihood, these levels are:

- **Unlikely**: Adversary is highly unlikely to initiate the threat event.
- **Likely**: Adversary is somewhat likely to initiate the threat event.
- **Very likely**: Adversary is almost certain to initiate the threat event.

With respect to impact, the identified levels are:

- **Not critical**: If the threat event is initiated or occurs, it is highly unlikely to have adverse impacts.
- **Significant**: If the threat event is initiated or occurs, it is somewhat likely to have adverse impacts.
- **Critical**: If the threat event is initiated or occurs, it is almost certain to have adverse impacts

Once both likelihood and impact are clearly evaluated, we can map their combination to a risk score, with values low, medium and high risk, according to the following risk score matrix:

TABLE 13 Risk score matrix

Likelihood \ Impact	Not critical	Significant	Critical
Unlikely	**Low**	**Low**	**Low**
Likely	**Low**	**Medium**	**Medium**
Very likely	**Low**	**Medium**	**High**

The association of each threat to certain risk score allows to sort them, and therefore, to prioritize those with a higher risk measure.

This is the final phase of the threat analysis, which includes some recommendations in order to minimize the risks associated to the studied tools (more on the security threat analysis methodology can be found in appendix 9.6).

5.2 Security Threat Analysis of the A4Cloud Tools

In this section we describe the results of applying the methodology described previously for each of the selected tools. For the sake of clarity, we focus here on the consolidated results that gather all threats. The actual threat models that led to these results are presented in the Appendix 10.3.

Once the threat models for each tool are defined, and specific threats are identified, we perform an expert evaluation on each of them in order to estimate the threats' impact and likelihood, and ultimately, to compute a risk score. The following table presents the results of this part.

TABLE 14 Identified threats' impact and likelihood

ID	Threat Name	Likelihood	Impact	Risk score
T1.1	Attacker may impersonate data subject through DT Frontend	Likely	Critical	High
T1.2	Attacker may tamper with encrypted data in DT Local Storage	Unlikely	Not critical	Low
T1.3	Attacker may tamper with DT communications	Unlikely	Not critical	Low
T1.4	Attacker can perform actions without being logged	Likely	Not critical	Low
T1.5	Attacker may access encrypted DT Local Storage	Unlikely	Critical	Medium
T1.6	Attacker may read DT communications	Unlikely	Significant	Low
T2.1	Attacker may impersonate TL Sender using his credentials	Unlikely	Critical	Medium
T2.2	Attacker may impersonate TL Receiver using his credentials	Unlikely	Critical	Medium
T2.3	Attacker may saturate TL Sender service	Very likely	Not critical	Medium
T3.1	Attacker may impersonate auditor through AAS Frontend	Likely	Critical	High
T3.2	Attacker may tamper with AAS communications (e.g., agents)	Unlikely	Significant	Low
T3.3	Attacker may access encrypted Evidence Store	Unlikely	Critical	Medium
T3.4	Attacker may read AAS communications (agents)	Unlikely	Significant	Low
T3.5	Attacker may saturate Evidence Store server (e.g., acting as agents)	Likely	Not critical	Low
T3.6	Attacker can perform actions without being logged	Likely	Not critical	Low
T4.1	Attacker may impersonate auditor through IMT Frontend	Likely	Significant	Medium
T4.2	Attacker can perform actions without being logged	Likely	Not critical	Low
T4.3	Attacker may saturate IMT server	Likely	Not critical	Low
T5.1	Attacker may read customer details	Likely	Not critical	Low
T5.2	Attacker may saturate DPIAT server	Likely	Not critical	Low
T6.1	Attacker may impersonate privacy administrator through DPPT Frontend	Likely	Critical	High
T6.2	Attacker can perform actions without being logged	Likely	Not critical	Low
T6.3	Attacker may saturate server	Likely	Not critical	Low
T7.1	Attacker may impersonate data subject through DT Frontend	Likely	Not critical	Low

T7.2	Attacker may saturate server	Likely	Not critical	Low

The following table shows a summary of the threats according to risk score.

TABLE 15 Summary of threats according to risk score

Risk Score	Number and percentage of threats
Low	16/25 (64%)
Medium	6/25 (24%)
High	3/25 (12%)

5.3 Conclusions

In the last table we can observe that most of the identified threats can be categorized as low risk, either because the impact is low or they are unlikely. On the other hand, only three of them are categorized as high risk. All the three threats rated as high-risk are actually instances of the Spoofing category of threats. In particular, these threats are associated to the Data Track, the Audit Agent System and the Data Protection Policies Tool. The rationale behind this fact is clear: these are critical tools, with user interactions through a credential-protected frontend. Therefore, spoofing attacks are potentially damaging the system since they allow access to crucial assets (data subjects' data in the Data Track, management of audit agents and records in the AAS, and management of policies in the DPPT). Apart from these threats, others categorized as medium risk are also of this type. It is then of vital importance that proper countermeasures are in place to prevent this type of threats, such as the use of multi-factor authentication and strong password policies.

The rest of threats are categorized either as medium or low risk, and basically are related to:

- Denial of Service (DoS) in the case of public APIs on server-based tools. This type of threat is very likely, but at the same time the associated impact is very low. Since most of the tools depend at some moment on a server-based component, it is recommended that proper mitigation to DoS attacks is in place.
- Tampering with encrypted data (possible if not using integrity mechanisms and/or using encryption modes of operation that do not provide authenticity/integrity). This type of attacks is technically more difficult to implement, and therefore, unlikely. The countermeasure is to follow appropriate practices (e.g, using authenticated encryption when possible)
- Trying to read encrypted data (minor threat, but possible once credentials are compromised)

Another interesting finding of this threat analysis is the identification of a subset of tools with an overall very low risk score:

- Data Protection Impact Assessment Tool (DPIAT)
- Redress and Remediation Tool (RRT)
- Incident Management Tool (IMT)

These tools practically do not add any representative threat to the interested stakeholders, but, on the contrary, provide accountability and data protection functionalities.

The rest of tools are more balanced, although they require to put in place certain security measures (such as the protection of users' credentials), which does not differ too much from typical IT applications that also require the implementation of common security practices. Overall, we conclude that the set of tools of A4Cloud results in a "positive sum", in the sense that accountability and privacy protection is enhanced by the tools, while security and functionality does not decrease or to a very low extent.

6 Near future impact scenarios

The data gathered via the interviews, the questionnaires, security threat analysis and relevant literature is used as input for the development of three impact scenarios. In these scenarios we address the question of anticipated ethical, legal and social dynamics in the practice of accountability in cloud ecosystems. Note, these scenarios are fictional narratives that describe plausible interactions between new technologies (the A4Cloud tools), society ('incidents' that drive privacy and data protection awareness), expected business models, and normative outlooks, including potential future ethical controversies. These scenarios provide a tool for anticipating the likely acceptance of accountability (tools) in the cloud ecosystem, for exploring the dynamics of interaction between current morality and new technologies, and for outlining the governing (market, law, social norms, architecture) mechanisms at play [38]. It is also possible to use the scenarios to formulate key incentives for stimulating accountability in the cloud (see next chapter).

The following three scenarios depict what the cloud ecosystems might look like in the near future (approximately 3 years from now):

a) The ideal of cloud computing,
b) The drivers of cloud computing,
c) Current governance of cloud computing,
d) Incidents that make problems with cloud computing visible,
e) Society's interest in cloud computing, and
f) Security in cloud computing.

6.1 In 3 years' time accountability is talk, but no action

There's a difference between talking about responsible handling of data and actually acting as a responsible data steward. Though discourse about data protection and security of cloud services has changed over the last three years, most CSPs and cloud customers are not yet willing to put their money where their mouth is. For example, secure data protection is agenda topic at board level, yet the number of CISOs or DP officers in the cloud ecosystem have remained marginal. Importantly, while more stakeholders acknowledge the importance of being able to demonstrate one complies with current data protection regulation, they also find that functionality of the cloud services outweighs responsible data stewardship. In other words, the expected RoI for accountability in the cloud ecosystem is too low. Of course, there are some CSPs and cloud customers that do follow their own more privacy friendly and data protection oriented approach. Yet, their influence on the entire cloud ecosystem to adopt a similar approach is relatively low. In addition, the general public does not add any pressure to cloud ecosystems to change their behaviour towards data and accountability. Subsequently, being a responsible data steward does not add much to a CSP's or companies' reputation. After the Snowden revelations no significant incidents have occurred that put privacy or data protection to the fore in social media or the news. In contrast, Western societies have been confronted with multiple terrorist attacks that have paved the way for legislation and European societal movements that press for more security and consequently often less privacy. While the GDPR implementation phase has been finalized a year ago, the European and national data protection authorities have received few resources to enforce the data protection legislation. Technological developments supporting accountability, such as the A4Cloud tools, have not been able to convince potential users of the lucrative business model that accountability could provide. Most accountability tools fail to meet both sector-specific implementation criteria and general feasibility. Though their general functionality is appreciated, the main governance mechanism driving the cloud computing industry remains the market and it's strive for innovation with limited restrictions by legal stakeholders.

6.2 In 3 years' time accountability is some talk and some action

Importantly after its (likely) enactment Spring 2016, the GDPR had a follow-up 2-year implementation phase. The enactment of the GDPR encouraged many cloud stakeholders to use the implementation phase for establishing minimal requirements necessary for complying with the regulation. Yet, most companies require more time than the two years provided for in the legislation. As a result most cloud stakeholders have taken *some action* to be able to demonstrate compliance with DP regulation, but

also have a rather reactive attitude towards its enforcement by European and national DP authorities. Especially enterprises and CSPs that are not digitally native struggle with how to combine the old and the new IT infrastructures within their companies at a time when IT budgets are also decreasing. In practice this means that the cloud ecosystem has not fully adopted the accountability notion as intended by the A4Cloud project, but organizational changes and adaptation of IT infrastructure towards more transparency about data whereabouts has become the norm. Simultaneously, it appears that some of the demands in the GDPR are quite difficult to achieve in practice. Auditing of metadata questions, for example, prohibit companies for fully complying with the GDPR. Moreover, some of the accountability tools developed in the A4Cloud project, such as COAT and DPIAT have been adopted by several organizations to facilitate responsibly making choices with respect to what cloud relations to engage in and what projects require what kind of data protection actions. Whereas these accountability tools are perceived to fill in the need of demonstrating good intentions, they are not yet widely embraced in the cloud ecosystem. The driving force in the socio-economic landscape remains the market governance mechanism and its push for innovation, yet increasingly the importance of guidelines and frameworks within the cloud ecosystem are recognized. CSPs certification by an independent certification agency has gained importance for cloud customers to prove trustworthiness and data protection and privacy not only are part of the board's meetings, yet increasingly become part of businesses codes of conduct. Nevertheless, the actual operationalization of these initiatives remains difficult given the dominant market mechanism. Even if CSPs are willing to increase accountable behaviour towards data in the cloud, the business model supporting this shift is deemed to be rather minimal, simply because their customers have low interest in giving up functionality for more laborious data protection procedures. Consumers' wishes for increased cloud mobility, as well as their expectations that corporate IT delivers quickly, with high usability, remain top drivers in the cloud ecosystem, often bypassing or ignoring the need for data protection.

6.3 In 3 years' time accountability is both talk and action

Societal appraisal of privacy and data protection has increased in the last three years due to new incidents of data leakage and privacy infringing activities in the cloud reported by social media and the press. Moreover, the public sector has taken up its responsibility to become a role model for privacy aware and responsible data stewardship. The private sector has gained notice of the privacy minded culture in the public sector and is picking up on best practices. Most of the leading companies in demonstrating 'responsible data stewardship' have focused on building more privacy-minded business models prior to the GDPR's adoption. In fact, they have used the concept GDPR as a blueprint for accountable behaviour with data despite uncertainty of its adoption. These frontrunner (often larger) companies have perceived privacy to be a unique selling point. Because they started altering their organizational and IT architecture in 2010 or soon thereafter towards more privacy minded models, they maximally profited from their reputation as trustworthy CSPs or cloud customers compared to other companies. Their examples of privacy friendly and profitable business models have paved the way for digitally native companies to follow their lead. Similar to the rise of the IT departments in the late '90s, more and more companies (both CSPs and cloud customers) are adopting Cloud and Future Internet adoption guidelines in order to warrant for secure and trustworthy data handling in the cloud. Not only has awareness increased, technological innovations, for example in the form of accountability tools that enable auditing according to GDPR regulations, and better understanding of how to handle metadata questions support a more accountable approach to data handling in the cloud. The market mechanism governing cloud computing is now interacting with other mechanisms such as law and social norms, balancing the drive for innovation with regulations for proper data handling and a responsiveness to societal and customers' demands.

6.4 Reflection on near future impact scenarios

A business case can help decision-makers assess the financial impact of deploying an accountable cloud architecture in the private sector, and the prices that are acceptable in the current market conditions and the projected future market. Part of a SEIA includes developing a number of plausible alternative scenarios that help identify different possible futures and the relative effects of these different impact scenarios (see section 2.1.2.1). The purposes of this chapter is not to predict which of the three alternatives is more or less likely, but rather to show how small changes to social, economic or legal factors can significantly influence the core social impacts related to accountability in the cloud.

Essentially, all three near-future impact scenarios presented here are equally plausible. It is therefore important to anticipate changes to the drivers and governance of cloud computing and how these might influence social interest, ideals and norms. Anticipating different alternatives enables formulating appropriate responses to different factors in practice. In the next chapter, we use the key factors from the scenarios to outline recommendations that enable policy responses that can be effective regardless of which type of alternative scenario plays out in the near future.

7 Recommendations

This final chapter will focus on how to proceed with the developed A4Cloud framework and tools in the near future. The scenarios in the previous chapter sketch potential futures and provide indications of how and where to stimulate the acceptance of accountability in the cloud ecosystem. That further stimulation of such acceptance is necessary is quite obvious. Our analysis of the accountability tools and interviews demonstrates the importance of proceeding with developments in this area. Accountability in the cloud ecosystem is not only believed to address customers' needs and demands, but also to become very profitable for CSPs. Yet, further development of accountability acceptance depends on various components: the perceived usefulness of accountability, internal organizational characteristics and external organizational characteristics. We outline and briefly explain 6 primary recommendations regarding further incentives for increasing the socio-economic impact of accountability in the cloud in the near future.

I. Enforcement of data protection and accountable behaviour is necessary

In order for accountability to be picked up by cloud ecosystem' stakeholders, the enforcement of responsible data stewardship should have taken concrete shapes. The two most likely methods for enforcement are: a) equipping European and national data protection agencies with sufficient measures to enforce compliance to the GDPR and b) create or enable an independent private organization to enforce good quality certification processes of 'responsible cloud service providers' as part of self-regulation by the sector. The legal enforcement of the (soon to be enacted) GDPR is a crucial and dominant factor in all three scenarios depicted in the previous chapter. However, except for legal recommendations as provided in for example Deliverable D-4.5 [49] and the white paper on contracts currently being written, few activities can be undertaken by A4Cloud to further stimulate the acceptance and adoption of the A4Cloud model and tools in the cloud ecosystem.

II. Facilitate independent auditing of responsible data stewardship

While enforcement of the GDPR is out of the control of the parties involved in A4Cloud, some influence on the independent private supervisory institute envisioned in previous A4Cloud work [31] to stimulate responsible data stewardship is more likely (see recommendation II). Especially since CSA is a partner within the A4Cloud project and also seems to resemble the previously described necessary organ for a certification mechanism very much. Respondents indicated that outsourcing of auditing and certification schemes is desirable from both cloud customers' and CSPs' perspectives. Independent auditing for responsible data stewardship, especially for SMEs, is often difficult to facilitate or achieve. As such, the frequency and relevancy of conducted audits (often by CSPs themselves) is questionable. Introducing an independent supervisory authority could facilitate in such auditing. The STAR (Security, Trust & Assurance) certification scheme that recently (September 2013) has been developed by CSA allows for credibly implementing certified/not certified decisions, and drastically reduces the technological complexity faced by users, which boosts trust in cloud services. While all eyes currently seemingly directed at the GDPR in relation to accountability, A4Cloud and CSA could further stimulate accountable behaviour in the cloud by redirecting some of the enforcement expectations by cloud stakeholders to the CSA and its system. Further research should demonstrate whether and how recommended adoption of A4Cloud's accountability model and accountability could somehow be (further) integrated in the STAR certification scheme.

Yet, also national initiatives such as the Quality Mark Zeker-°©-OnLine "an independent, transparent Quality Mark for online accounting services (also referred to as 'cloud accounting solutions')" can increase the adoption of accountability in cloud ecosystems. Zeker-°©-OnLine "was developed following an initiative taken by the Tax and Customs Administration, the providers of online accounting services and the Electronic Commerce Platform Nederland (ECP) that was intended to provide a quality guarantee for the users of accounting services. This initiative resulted in the definition of quality requirements that have been specified in a framework of standards" [6]. Local initiatives such as these can and should be supported by A4Cloud partners whenever the opportunity arises in order to further stimulate the use of accountability mechanisms in cloud ecosystems.

III. Increase awareness of the need for accountability

In general, social awareness of the need for accountability thus far seems rather low. Whereas the expert interviews demonstrated high interest in accountability, the lack of response to surveys

[6] https://www.zeker-online.nl

distributed via A4Cloud's network, and the type of responses by the panel members may demonstrate a lack of awareness on the part of not only CSPs and cloud customers but also the public at large. First, the current cloud ecosystem seems to lack standardized and supported guidelines or a supported code of ethics for responsible data stewardship. A4Cloud's accountability legacy and framework offer tools for writing a non-legal white paper (next to the legal white paper in progress) or initial set-up of new 'codes of ethics' for the cloud. Therefore, A4Cloud should take the initiative in developing such a code of ethics and guidelines creating awareness and stimulating accountable behaviour by CSPs. Second, by (freely) offering tools like COAT and DPIAT to cloud customers, a conditional framework or guidelines for establishing trustworthy or responsible relationships with CSPs is provided. By using these tools, cloud customers simultaneously use a market governance mechanism to select the best CSPs for the job and are pointed at the potential risks attached to using cloud services. Again, A4Cloud's accountability legacy can offer a structure for the formulation of such guidelines. Third, stimulating awareness in the general public is not easily done via EU-projects and largely depends on incidents receiving media attention. However, in the flow of relevant media coverage, A4Cloud could 'market' tools such as Data Track to the general public. Stimulating the use of the Data track tool by laymen likely increases their awareness of the whereabouts of their personal data in the cloud and subsequently of the need for accountability mechanisms and tools in the cloud. Last, pointing out the existence of certification schemes or quality marks (see recommendation II) to both business cloud customers and individual cloud customers is part of raising awareness.

IV Balancing the information asymmetry via partnerships

Another way for stimulating accountability in the cloud, the information asymmetry between CSPs and cloud customers should become more balanced. Though the knowledge gap is quite large and will not necessarily be resolved within the short term, SMEs can take actions. A best practice example is SURF, the collaborative ICT organisation for Dutch higher education and research. The collaboration between various ICT organisations in one foundation has given these organizations sufficient body to become a meaningful discussion partner for larger CSPs. Whereas A4Cloud can only recommend cloud customers to join forces, it can also provide cloud customers some tools, such as COAT and the Transparency Log, which would enable them to become more equal partners in, for example, contractual deliberations.

V. Focus on larger enterprises working in the public sector first

Importantly, good examples tend to be followed. Previous research within A4Cloud already demonstrated that "ethical accountability assumes that an intrinsic need and value of accountability will strengthen cloud providers and business cloud users' position in the market. Incorporating the mechanisms and practices of ethical accountability, based upon the notions of sustainability and inclusion, in the cloud eco-system could result in an active competition between organizations to be known (or labelled) as ethically accountable organizations. Moreover, the modelling demonstrates how ethically accountable service providers can have a significant positive effect on the trustworthiness of the entire ecosystem" [31]. Whereas the A4Cloud project predominantly focused on developing an Accountability framework for SMEs and smaller CSPs, it appears that these smaller organisations often lack the resources (both in money and personnel) to actually pursue such responsible stewardship. In essence, smaller companies seem to focus on functionality above accountability of cloud services. However, the organisations that not only talked about accountability but also acted as responsible data stewards seem more likely to be larger (hence having resources) and also to work in the public sector. Especially CSPs working in the healthcare domain or in domains in which sensitive or personal data is processed seem more likely to have internal organizational characteristics that reflect a tendency towards good governance of data. Therefore, A4Cloud could identify larger companies within these sectors and start promoting material to them. As soon as these enterprises seem to adopt the A4Cloud framework and tools, they can become showcases of 'best practices' for the A4Cloud project results. Since the A4Cloud project already includes larger companies they also should provide for these showcases themselves.

VI. Demonstrate how A4Cloud tools and mechanisms can be turned into a business model

Most importantly, A4Cloud should demonstrate how the accountability framework and tools offer profitable business models. Previous work within A4Cloud (see [31]) already demonstrated how embedding accountability practices that go beyond minimal accountability requirements within one's organisation actually improves the health and sustainability of the cloud ecosystem. It facilitates better recovery of the entire cloud ecosystem after incidents due to the increased trustworthiness of accountable organisations. Current work demonstrates that privacy and data protection are

increasingly seen as marketable unique selling points. Hence, highlighting the importance of a good reputation to CSPs and pointing customers toward existing certification schemes and best practices of accountable behaviour likely increase the cloud computing market's interest in accountability business models. Importantly, the current formulation of the A4Cloud tools does not yet support the provision of a clear and profitable business model for potentially interested cloud stakeholders, for three reasons. First, the accountability notion remains a vague and complex notion. However, its deconstruction in tangible and concrete main features (including, for example, compliance to GDPR, transparency for cloud customers, and information about, for example, data whereabouts and data leakages) makes the accountability notions more concrete. Second, current descriptions of the tools are too scientific and do not relate to everyday practice in the cloud business markets. The descriptions need to address business-relevant problems such as security and contracts, not scientific validity. Third, it is questioned by the potential users whether the tools fit specific sectors and hybrid IT infrastructures. A4Cloud should, for example, demonstrate how A4Cloud tools are suitable for both digitally native and digitally non-native companies.

8 References

[1] M. G. Niezen and W. M. Steijn, “Understanding the Cloud: The Social Implications of Cloud Computing and the Need for Accountability,” in *Accountability and Security in the Cloud*, Springer, 2015, pp. 201–225.

[2] F. Vanclay, “International principles for social impact assessment,” *Impact Assess. Proj. Apprais.*, vol. 21, no. 1, pp. 5–12, 2003.

[3] F. Vanclay and A. M. Esteves, *New directions in social impact assessment: conceptual and methodological advances*. Edward Elgar Publishing, 2011.

[4] Bureau of Rural Sciences, “Socio-economic Impact Assessment Toolkit: A guide to assessing the socio-economic impacts of Marine Protected Areas in Australia, Australian Government Bureau of Rural Sciences.”

[5] S. Coles, “Practitioner perspectives on the barriers and constraints to the assessment of socio-economic impacts in EIA,” 2007.

[6] A. A. G. TIWARI, “A Handbook for Socio-economic Impact Assessment (SEIA) of Future Urban Transport (FUT) Projects.”

[7] Mackenzie Valley Environmental Impact Review Board, “Socio-Economic Impact Assessment Guidelines,” 2007.

[8] Z. Juan, J. Wu, and M. McDonald, “Socio-economic impact assessment of intelligent transport systems,” *Tsinghua Sci. Technol.*, vol. 11, no. 3, pp. 339–350, 2006.

[9] A. Passani, F. Monacciani, S. Van Der Graaf, F. Spagnoli, F. Bellini, M. Debicki, and P. Dini, “SEQUOIA: A methodology for the socio-economic impact assessment of Software-as-a-Service and Internet of Services research projects,” *Res. Eval.*, vol. 23, no. 2, pp. 133–149, 2014.

[10] J. Droff and A. R. Paloyo, “Assessing the regional economic impacts of defense activities: A survey of methods,” *J. Econ. Surv.*, vol. 29, no. 2, pp. 375–402, 2015.

[11] G. Dalton, G. Allan, N. Beaumont, A. Georgakaki, N. Hacking, T. Hooper, S. Kerr, A. M. O’Hagan, K. Reilly, and P. Ricci, “Economic and socio-economic assessment methods for ocean renewable energy: Public and private perspectives,” *Renew. Sustain. Energy Rev.*, vol. 45, pp. 850–878, 2015.

[12] K. Malone, “Socio-economic impact assessment for driver assistance systems,” *FESTA Deliv.*, vol. 2, 2008.

[13] M. Edwards, “Community guide to development impact analysis,” *Madison WI Univ. Wis.-Madison*, 2000.

[14] J. Rolfe, G. Ivanova, and S. Lockie, “Assessing the social and economic impacts of coal mining on communities in the Bowen Basin: summary and recommendations,” *Mackay QLD Cent. Environ. Manag. CQU*, 2006.

[15] J. Halim Nauckhoff and P. Fentsch, “Sustainable Infrastructure Development-A Socio-economic Impact Analysis of Airport Development in Vietnam,” 2013.

[16] W. M. Steijn and M. G. Niezen, “The Value of Accountability in the Cloud: Individual Willingness to Pay for Transparency,” *Technol. Soc. Mag. IEEE*, vol. 34, no. 4, pp. 74–82, 2015.

[17] F. D. Davis, R. P. Bagozzi, and P. R. Warshaw, “User acceptance of computer technology: a comparison of two theoretical models,” *Manag. Sci.*, vol. 35, no. 8, pp. 982–1003, 1989.

[18] V. Venkatesh and F. D. Davis, “A theoretical extension of the technology acceptance model: Four longitudinal field studies,” *Manag. Sci.*, vol. 46, no. 2, pp. 186–204, 2000.

[19] E. M. Rogers, *Diffusion of innovations*. Simon and Schuster, 2010.

[20] P. A. Pavlou, “Consumer acceptance of electronic commerce: Integrating trust and risk with the technology acceptance model,” *Int. J. Electron. Commer.*, vol. 7, no. 3, pp. 101–134, 2003.

[21] McKnight, “Trust in Information Technology,” in *The Blackwell encyclopedia of management*, vol. 7, Malden, MA: Blackwell Pub, 2005, pp. 329–331.

[22] S. Pearson and G. Yee, *Privacy and security for cloud computing*. Springer Science & Business Media, 2012.

[23] A. Baldwin, D. Pym, and S. Shiu, “Enterprise information risk management: Dealing with cloud computing,” in *Privacy and Security for Cloud Computing*, Springer, 2013, pp. 257–291.

[24] D. H. McKnight, V. Choudhury, and C. Kacmar, “Developing and Validating Trust Measures for e-Commerce: An Integrative Typology,” *Inf. Syst. Res.*, vol. 13, no. 3, pp. 334–359, Sep. 2002.

[25] A. de Oliviera, A. Garaga, L. A. Martucci, M. Felici, R. Alnemr, D. Stefanatou, M. Niezen, C. Fernandez, D. Nuñez, B. Hasnain, A. Vranaki, and E. Cayirci, “D:C-6.1: Risk and trust accountability in the cloud,” SAP, 2014.

[26] M. Felici and S. Pearson, “Conceptual Framework,” Bristol, DC32.1, 2014.

[27] M. G. Jaatun, S. Pearson, F. Gittler, and R. Leenes, “Towards Strong Accountability for Cloud Service Providers,” in *Cloud Computing Technology and Science (CloudCom), 2014 IEEE 6th International Conference on*, 2014, pp. 1001–1006.

[28] F. Gittler and T. Koulouris, “D:D-2.2a: High-level architecture,” HP Labs, 2014.

[29] A. Osterwalder and Y. Pigneur, *Business model generation: a handbook for visionaries, game changers, and challengers*. John Wiley & Sons, 2013.

[30] M. Niezen, P. Prüfer, R. E. Leenes, D. Nuñez, I. Agudo, C. Fernandez Gago, T. Koulouris, and R. Alnemr, “A4Cloud D:B-4.1 Interim report,” Tilburg University, TILT, 2013.

[31] M. G. H. Niezen, W. M. P. Steijn, R. Alnemr, T. Koulouris, S. Høyland, D. Nunez, Fernandez Gago, and R. E. Leenes, “A4Cloud: Final report on socio-economic context,” Tilburg, D24.2, 2014.

[32] TechSoup Global Network, “Global Cloud Computing Survey Results.” 2012.

[33] Microsoft | TechNet, “Cloud computing survey. The results.” 2011.

[34] KPMG, “The cloud takes shape. Global cloud survey.,” 2013.

[35] P. Mell and T. Grance, “The NIST definition of cloud computing,” 2011.

[36] F. Etro, “The economic impact of cloud computing on business creation, employment and output in Europe,” *Rev. Bus. Econ.*, vol. 54, no. 2, pp. 179–208, 2009.

[37] V. De Pous, “Cloud Computing & Public Sector Policy. The case for doing more with less and innovate public administration start with cloud policies. An executive analysis.,” 2012.

[38] L. Lessig, *Code*. Lawrence Lessig, 2006.

[39] OECD, “The OECD Privacy Framework.” OECD, 2013.

[40] A.-P. E. Cooperation, “Apec privacy framework,” 2004.

[41] Tableau, “Top 10 Cloud trends for 2016.” 2015.

[42] M. Bovens, “Analysing and assessing public accountability: a conceptual framework,” 2006.

[43] C. Hood, “Accountability and Transparency: Siamese Twins, Matching Parts, Awkward Couple?,” *West Eur. Polit.*, vol. 33, no. 5, pp. 989–1009, Aug. 2010.

[44] C. J. Bennett, “International Privacy Standards: can Accountability be Adequate?.”,” *Priv. Laws Bus. Int.*, vol. 106, pp. 21–23, 2010.

[45] OWASP, “OWASP Application Threat Modeling.” .

[46] M. S. Lund, B. Solhaug, and K. Stølen, *Model-driven risk analysis: the CORAS approach*. Springer Science & Business Media, 2010.

[47] Microsoft, “SDL Threat Modeling Tool.” .

[48] E. A. Nist, “NIST Special Publication 800-30 Risk Management Guide for Information Technology Systems,” *Creat. Paramount CA*, 2012.

[49] C. Reed and D. Stefanatou, “D:D-4.5 Report on Legal and Regulatory Dependencies: embedding accountability in the international legal framework,” D-4.5, 2015.

[50] A. E. Boardman, D. H. Greenberg, A. R. Vining, and D. L. Weimer, “Cost-benefit analysis: concepts and practice,” 2006.

[51] D. van Woensel, M. G. H. Niezen, and S. Adams, “A4Cloud. Internal report on SEIA model developed,” Tilburg, Internal milestone MS:A-4.1.

[52] T. Buchanan, C. Paine, A. N. Joinson, and U. Reips, “Development of measures of online privacy concern and protection for use on the Internet,” *J. Am. Soc. Inf. Sci. Technol.*, vol. 58, no. 2, pp. 157–165, 2007.

9 Appendices

9.1 Overview of initial hits, literature review

TABLE 16 Literature review search method

Database	Search term	Search type	Hits	Relevant hits
Econpapers	Socio economic impact assessment	Advanced search - free text search - sorted on rank	460036	13 (of first 200 results)
	Socio economic AND impact assessment	Advanced search - free text search - sorted on rank	57266	7 (of first 40 results)
	"Socio economic impact assessment"	Advanced search - free text search - sorted on rank	10	4
JStor	Socio economic impact assessment	Normal search	62231	4 (of first 100 results)
	Socio economic AND impact assessment	Normal search	41	1
	"Socio economic impact assessment"	Normal search	9	7
HeinOnline	socio economic impact assessment	Normal search	295	1
	"Socio economic impact assessment"	Normal search	28	11
	"Socioeconomic impact assessment"	Normal search	3	2
JStor	Socio economic impact assessment	Normal search	62231	4 (of first 100 results)
	Socio economic AND impact assessment	Normal search	41	1
	"Socio economic impact assessment"	Normal search	9	7
ScienceDirect	Socio economic impact assessment	Normal search	48231	50
	"Socio economic impact assessment"	Normal search	78	7
Taylor & Francis Online	Socio economic impact assessment	Normal search	64895	50
	"Socio economic impact assessment"	Normal search	48	10
CiteSeer	"Socio economic impact assessment"	Normal search	211	11
	"Socio-economic impact assessment"	Advanced search - Title	3	1
Worldcat	"Socio economic impact assessment"	Normal search	436	118
Google Scholar	Socio economic impact assessment	Normal search	840000	5
	"Socio economic impact assessment"	Normal search	1920	12

	Socio economic impact assessment method	Normal search	584000	6
Google	Socio economic impact assessment handbook	Normal Search	3540000	6 (of first page)

9.2 Oversight A4Cloud tools developed

TABLE 17 Accountability tools developed by A4Cloud

A4Cloud tools	Main user	What
Cloud Offering Advisory Tool (COAT)	Cloud customer (SME)	Contract & Risk Management. Contract support tool: enable cloud (end) users to make choices **Informed choice**
Data Protection Impact Assessment Tool (DPIAT)	Cloud customer (SME)	Contract & Risk Management. Performing mandatory impact assessment for cloud customer. Enable cloud (end) users to make choices **Informed choice**
Data Protection Policies Tool (DPPT)	CSP	Implementing Policy / Policy definition and enforcement Create machine readable privacy policy Create technical representation of the policy Configure the enforcement engine (APPL-E) **Control and transparency**
Accountablity Lab (AccLab)	CSP	Implementing Policy; policy definition and enforcement Checks compliance between customer desired privacy policy and cloud service offering **Control and transparency**
APPL Engine (APPL-E)	CSP	Incident Management; policy definition and enforcement Enforces data protection policies in SaaS provider Logs actions performed Sends incident notifications **Control and transparency**
Data Transfer Monitoring Tool (DTMT)	CSP	Incident Management; evidence Detects violations of data transfer policy in infrastructure service **Compliance**
Incident Management Tool (IMT)	CSP	Incident Management; remediation. Provides user interface for security expert to check incident related events **Compliance**
Audit Agent System (AAS)	Auditor	Monitoring and Audit; evidence. Audits actions through logs received Detects policy violations **Compliance**
Transparency Log Tool	Auditor	Monitoring and Audit; data subjects control Secure and privacy preserving tool to send logs throughout the cloud environment **Control and transparency**
Data Track (DT)	Cloud subject	Data subject controls. Gives cloud subject visibility of which services are collecting data and of what data is

		stored in the cloud **Control and transparency**
Remediation and Redress Tool (RRT)	Cloud subject	Incident management & remediation Supports cloud subject taking appropriate action in response to incidents **Compliance**
Assertion Tool	Tool developers	Scenario-based validation of accountability tools

9.3 Questionnaire (design) socio-economic impact accountability tools

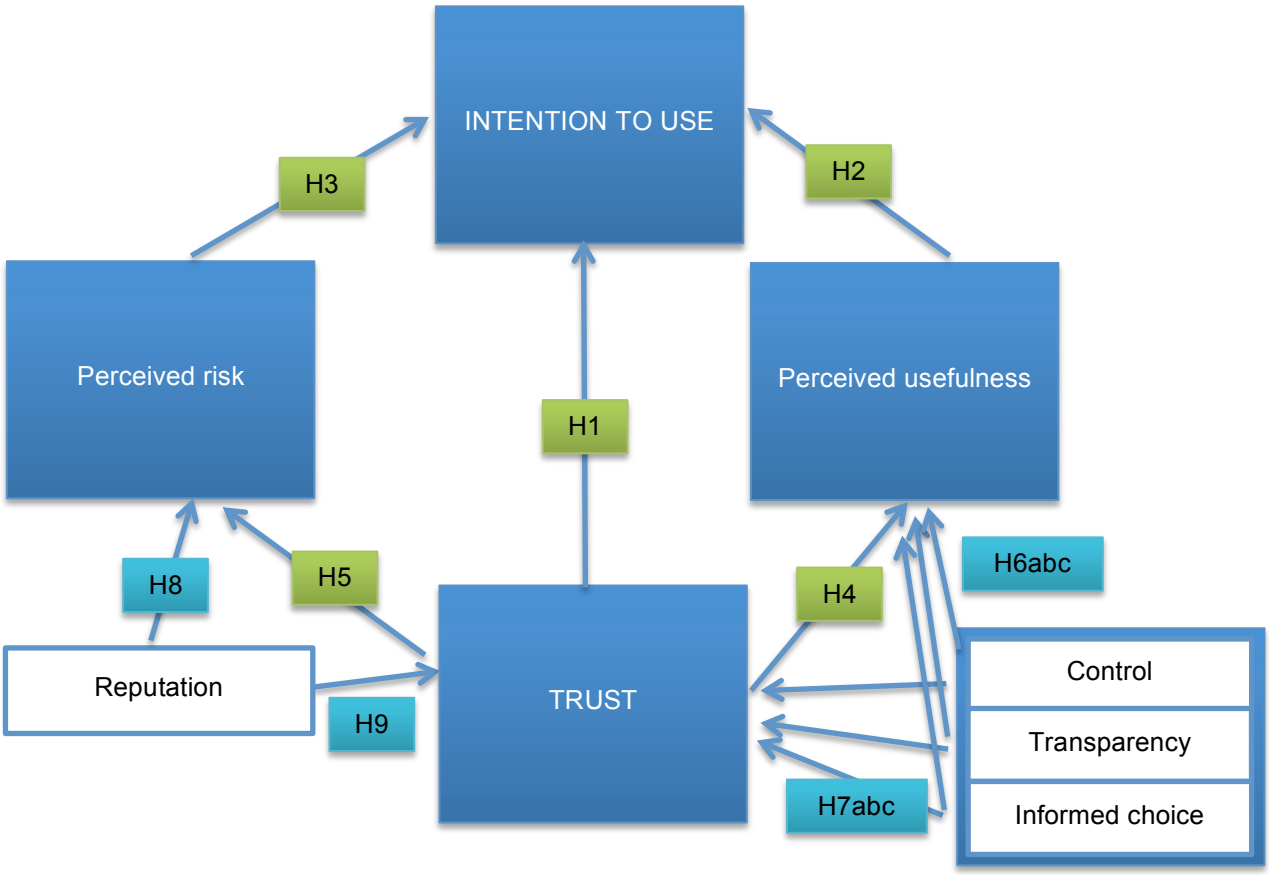

Figure 12 Hypotheses and model for questionnaire design

H2: Consumer's intention to use accountability tools is positively related to the perceived usefulness of these accountability tools

H3: Consumer's intention to use accountability tools is negatively related to consumer perceived risk

H4: Consumer trust is positively related to the perceived usefulness of these accountability tools

H5: Consumer trust is negatively related to consumer perceived risk

H6a: Consumer control is positively related to the perceived usefulness of accountability tools

H6b: Transparency is positively related to the perceived usefulness of these accountability tools
H6c: Informed choice is positively related to the perceived usefulness of these accountability tools

H7a: Consumer control is positively related to consumer trust
H7b: Transparency is positively related to consumer trust
H7c: Informed choice is positively related to consumer trust

H8: Reputation is positively related to consumer trust
H9: Reputation is negatively related to perceived risk

Questionnaire questions

Thank you for taking time to complete this survey. Your contribution is crucial to our research and is greatly appreciated! Tilburg University and SINTEF are conducting research on the socio-economic impact of accountability in the cloud as part of the EU funded Accountability for Cloud project (A4Cloud). We are interested in how you feel about tools that assist and stimulate responsible data stewardship in the cloud. A4Cloud's aim is to give cloud service users more control and transparency over how their data is used in the cloud and helping businesses to understand and manage the risks of putting data in the cloud. Over the last three years universities, companies (e.g. HP, SAP) and the Cloud Security Alliance have collaborated in A4Cloud to develop prototypes of potential accountability tools. We are interested in the value you attribute to the functionality of these prototypes. It will take approximately 10-15 minutes to complete the questions in this short survey. The switch to the first screen might take 10-20 seconds. More information on the Cloud Accountability Project (A4Cloud) can be found on: http://A4Cloud.eu.

Role in cloud infrastructure

Q0001

If I have to categorize myself, my main role(s) in cloud infrastructures is / are as:

Tick one box that suits your role best / main role.

- Data subject - It is my (organization's) data being processed in the cloud.
- Individual cloud customer - I am maintaining a business relationship with and using services from cloud service providers.
- Organizational cloud customer (SME) - I am (part of a small and medium enterprise) maintaining a business relationship with and using services from cloud service providers.
- Organizational cloud customer (LE) - I am (part of a large enterprise) maintaining a business relationship with and using services from cloud service providers.
- Cloud service provider - I am (part of an organization) making cloud services available to cloud customers.
- Cloud auditor - I am (part of an organization) conducting independent assessment of cloud services, information system operations, performance and security of the cloud implementation, with regards to a set of requirements, which may include security, data protection, information system management, regulations and ethics.
- Supervisory authority - I am (part of an organization) overseeing and enforcing the application of a set of (data protection) rules.

[no 'other' possibility]

Q0001b

What kind of function do you have?

- Business services / administration manager
- Sales, marketing and/or development manager
- Chief executive / managing director
- Security officer / quality and safety manager
- Office manager
- Professional staff

- Other

Q0001c

In what sector do the business transactions of your organization / company primarily take place?

- public sector
- private sector
- Equally in public and private sector
- Not applicable

[Respondents will be answering questions for a maximum of 5 tools. Hence descriptions slightly differ (i.e. in reference to other tools) per type of respondent (Q0001).

a) Auditor/supervisory author: DPPT, AAS, TL
b) CSPs: DPPT, IMT, AAS, TL. DT
c) Cloud customers (individual, SMEs/ LEs): DPIAT, DPPT, IMT, RRT
d) Data subject: TL, DT, RRT]

Functionality of accountability tools

Within A4Cloud several prototype accountability tools have been developed. Based upon your main role within the cloud infrastructure we would like to ask you some questions about relevant accountability tools and their main features.

Please read through the brief explanations of the 7 prototypes before answering the questions.

Data Protection Impact Assessment (DPIA) Tool The DPIA tool has a friendly web-based interface. It presents 2 questionnaires about the data protection measures for a given project: an initial screening and a subsequent full screening. These questionnaires are tailored to the needs of Small and Medium Enterprises (SMEs). The approach is based on legal and socio-economic analysis of privacy issues for cloud deployments and takes into consideration the proposed new requirements for DPIAs within the European Union (EU).

Data Protection Policies Tool (DPPT) The DPPT facilitates the joint specification and implementation of accountability policies between cloud customers and cloud providers/brokers/carriers. It creates a machine readable privacy policy and a technical representation of the policy that allows for (automatic) policy enforcement of data protection.

Incident Management Tool (IMT) The IMT is the entry point for handling anomalies and detected violations in cloud environment scenarios. This tool receives incident notifications from downstream providers or local A4Cloud tools, such as AAS. It also notifies upstream providers of incidents. In cases where incidents received by IMT affect end-users of this provider, IMT takes the initial steps to respond to these incidents by sending alerts. The IMT and RRT (see next description) are linked.

Remediation and Redress Tool (RRT) The RRT assists individual end users or small SME cloud customers in responding to (perceived) incidents in their cloud arrangements. The RRT is activated when certain incidents are reported by the Incident Management Tool (see previous description) or when it is invoked by the users on the basis of information collected from other sources. It lists possible actions that can be undertaken and will guide users through the actions.

Audit Agent System (AAS) The AAS is a tool for auditors and providers to use to verify the compliance with policies. It automatically and continuously collects and analyses evidence, and assures accountable execution of processes in the cloud.

Data Track (DT) tool The DT is a tool that gives data subjects an overview of all the personal data they have disclosed. This tool allows them to search through their data disclosure history. They can see what personal data they have disclosed, to whom and under which privacy policy.

Transparency Log (TL) tool TL provides a secure and privacy-preserving one-way communication channel between service providers and data subjects. Using TL, service providers can share more data with data subjects, including potentially privacy-sensitive data, which normally cannot be sent via for example email or SMS.

Q0002a, b, c, d

How would you rate the clarity of the following descriptions of the accountability tools?

- Good
- Fair
- Poor

Q0003a, b, c, d

The functionality of the following prototypes would likely be useful in my daily practice.

5-point-Likert, Completely(dis)agree, n.a. don't know

Q0004a, b, c, d

Using the following accountability tools would likely improve the quality of the work I do.

5-point-Likert, Completely(dis)agree, n.a. don't know

Q0005a, b, c, d

Compared to the tools I am currently using these tools seem more beneficial to enhance responsible data stewardship.

5-point-Likert, Completely(dis)agree, n.a. don't know

Q0006

I find being able to show others that I handle data (e.g. process, store) in the cloud in a responsible manner important.

5-point-Likert, Completely(dis)agree

Q0007a, b, c, d

Using these tools will likely improve my organization's reputation as a responsible data steward.

5-point-Likert, Completely(dis)agree, n.a. don't know

Q0008

To what extent does a reputation as responsible data steward have economic value for you / your company?

4-point scale (To a great extent, some extent, very little, not at all), I do not know.

Q0009a, b, c, d

How much effort would likely be needed to implement these tools in your daily practice?

4-point scale (Great effort, Some effort, Very little effort, No effort at all) I do not know.

Q0010

To what extent will the expected effort be a significant barrier for implementing the accountability tools?

4-point scale (To a great extent, some extent, very little, not at all), I do not know.

Organizational characteristics in relation to accountability

We are interested in your organization's attitude towards the need for accountability.

Q0011a, b, c

Please indicate for the organisation you represent your perception of the following elements:

- Data protection is important.
- My organization makes use of accountability measures to demonstrate responsible data stewardship.
- My organization needs to make changes due to the upcoming legislation with respect to data protection and privacy.
- The (top) management is likely to accept changes that accompany innovation.
- My organization has a strong hierarchical structure.
- Following existing practices, policies and protocols related to data protection and privacy is the norm.
- My organization consists of members/departments each having their own specialized knowledge and expertise.
- My organization has close ties with auditing or advisory institutes regarding data protection.

Q0012a, b, c, d

Please indicate your perception on the following statements.

5-point-Likert, Completely(dis)agree, n.a. don't know

- Information on how cloud service providers may use my data allows for better choices in the selection of cloud service providers. [a,c,]
- Based upon information from data protection impact assessments I am likely to change my choice in cloud service provider. [a,c,]
- I would pay for services that offer insight in how I am doing with respect to protecting data I am entrusted with. [a,b,c,]
- When a cloud service provider gives increased control over personal/sensitive data this encourages my usage of its services. [a,c]
- Automation of data protection/privacy policies provides more certainty on data protection. [a,b,c,]
- I would pay for services that offer control over how I am protecting data I am entrusted with. [a,b,c,]
- Transparency about specification and implementation of accountability policies adds value to the business process. [a,b,c,]
- Tools that provide individuals insight of their data disclosure history will increase the confidence that data is handled according to their expectations. [a,b,c,d]
- Auditors should be confident that data is communicated in a privacy-preserving way. [a,b,c,d]
- Data protection incidents should be reported to all relevant parties, including data subjects and cloud customers. [a,b,c,d]
- Damage due to data protection incidents should be remediated. [a,b,c,d]
- I only work with (other) cloud service providers I have worked with before. [a,b,c,]

Workshop

We will be holding additional (telephonic) interviews to study conditions for increased accountability in the cloud infrastructure. **May we contact you for an interview?** By answering yes and providing your contact information (please provide an email address only), you give the researchers consent to contact you between February 17th and March 31st, 2016.

Moreover, **March 7th 2016** A4Cloud organizes a **workshop on the A4Cloud tools and their expected impact** in Brussels, Belgium. If you are interested to join this workshop, feel free to indicate this.

Please choose all that apply and provide a comment:

Thank you for your participation.
Maartje Niezen (m.g.h.niezen@uvt.nl)
Børge Haugset

9.4 Topiclist TiU social impact

Background information respondent

Can you briefly introduce your company: i.e. number of employees, industry, sector, ownership, etc.?

What is your position and / or role in the company?

What is your company's / organization's relationship with cloud-based services?

What is your company's perception of the need for being accountable in relation to data protection (awareness of upcoming GDPR)?

Functionality of accountability tools

Please read through the brief explanations of the prototypes in preparation of the interview.

Would you, based upon the descriptions, understand what the tool could offer you?

Which of these tools would you likely use in your daily practice?

What about there functionality?

What are the main features of these tools?

- Trust
- Informed choice & transparency
- Control
- Compliance

To what extent do you believe these tools can improve the quality of your work?

What are your current efforts in being/becoming a responsible data steward?

Many companies already make use of privacy policies and other mechanisms to demonstrate they handle data responsible. What are the actions you undertake in relation to data protection? Can you give some examples?

How would you rate your employees' competence and willingness in adopting new tools like these?

As management, what actions do you take to ensure everyone adheres to your company's vision on data protection? / What actions are taken by the management to ensure everyone adheres to the company's vision on data protection?

Introduction of accountability and GDPR

For what reason would you start using tools or mechanisms that demonstrate responsible stewardship?

To what extent do you find the responsible handling of data of importance for your company from a marketing perspective?

To what extent do you find the responsible handling of data of importance for your company from a societal perspective?

To what extent is the upcoming GDPR reason to change current practices within your company?

9.4.1 Respondents

TABLE 18 Respondents interviewed by TiU

Respondent	Date interviewed	by	Cloud role

Carlo Daffara	07/03/2016	MN	CSP / SME / public & private sector
Andre Foeken	07/03/2016	MN	CSP / LE / public sector
Wouter Koenders	08/03/2016	MN	CSP / Cloud broker / SME / public & private sector
Corno Vromans	17/03/2016	MN	Cloud customer / LE / Public sector

9.5 Economic CBA method

The economic assessment has focused on identifying the potential pros (and cons) of the tools as identified by individual users and different business actors in the sky value chain. The approach of the economic assessment is based on a standard business model with respect to which elements are considered the most important for business [29]. The Cost-benefit method [50] complements the business model approach as a framework for the assessment.

Based on the current status of the accountability tools and information available, the approach of the Cost-Benefit Analysis serves as a conceptual framework for the economic assessment. As a point of departure, the CBA is often based on, and aims at broadening or complementing the scope of a financial analysis (which typically focus on profitability of a project or a measure). In this case, the actual project or measure to assess is a number of tools. To be more accurate, the scope is to assess the economic potential of the tools, primarily in a market setting, as market acceptance is a prerequisite for deployment. Nevertheless, the aim is to have a wider perspective than the financial approach offers. Accordingly, the CBA is relevant as general framework for taking into account positive and negative economic effects beyond what appear in the cash flow and accounts of the individual users and the cloud business enterprises.

The major steps in CBA are [50]:

1. Specify the set of alternative projects
2. Decide whose benefits and cost count (standing)
3. Catalogue the impacts and select measurement indicators
4. Predict the impacts quantitatively over the life of the project
5. Monetize all effects
6. Discount benefits and costs to obtain present values
7. Compute the net present value of each alternative
8. Perform sensitivity analysis
9. Make a recommendation

1: The set of alternatives to be assessed are the seven tools listed in Chapter 2. The baseline is the current situation, characterized with lack of similar tools and where manual and time consuming periodic reviews or processes appear to be the existing options (Chapter 3). Regarding aspects of the legal and regulatory status of cloud computing, we presuppose the status quo, with the exception that the announced EU GDPR will be enforced 2018.

2. A4Cloud tools are addressing individual and business end users as well as other business actors in the cloud computing value chain. The economic assessment is based on data gathered by the survey and a limited number of interviews. Accordingly, our work is based on information from individual and SME end users, a broker, which also delimit the generality of the results of the economic assessment.

3. The intended effects and gains of the tools for the individual targeted users and user groups are partly included in the tool description and more details are offered in chapter 4, which also offers a qualitative description of intended effects for the cloud business in general. Interviewees and survey respondents have made statements about benefits and impacts they expect, but not in a way enabling measurement indicators and predicting impact quantitatively. One reason for this is already indicated: Tool description is short and uncertainty regarding what the tools include and how they work seems apparent. Uncertainty about competing technology and tools, future markets and future framework adds to the complexity and of making quantitative impact assessments.[7]

[7] Thus, the baseline assumption of status quo was typically challenged by the interviewees

4, 5, 6, 7 and 8: As effects cannot be quantitatively predicted, monetizing and discounting, computing net present value (of costs and benefits) are not relevant. However, not being able to monetize effects is not unusual. To the contrary, the CBA textbook typically warns that it is not wise trying to estimate and monetizing effects without taking into account time and costs [50]. Accordingly, discussing effects within the CBA framework without monetizing is well accepted although the aim is to monetize. Besides, we will remark that quantitative estimates make effects appear to be both more accurate and credible than we think is reasonable taking into account the status of the tools and the prevailing uncertainty about benefits and costs and commercial interest. As monetizing and quantitative measures are not estimated, sensitivity analysis is not considered relevant.

9 The A4Cloud project is about developing, testing and demonstrating new technology. Economic, environmental and social sustainability analyses have been conducted, and recommendations are in demand. Making recommendations is in the CBA setting often interpreted as actually picking a "winner" or a few winners amongst a bigger set. However, in this case, making recommendations is much about presenting pro et cons and how to go on to improve the economic, environmental and social performance of the assessed alternatives. Multi Criteria methods (see milestone [51]) could have been applied as a basis for recommendations (especially as we have not been monetizing and proved unable to prioritize tools based on strict economic measures). However, utilizing the MC-methods for prioritizing tools will have added to the cost and the complexity of the analysis and not necessarily to transparency. Besides, lack of quantitative measures appear to be detrimental to transparency of recommendations based on multi criteria methods [52].

Importantly, in a fully fledged CBA-analysis one would typically (or it could be an option to) look more into issues related to improved personal data security and right to privacy in general, and elaborate on gains not adding to the actors cash-flows rather to the benefit of the public, citizenship and society in general. As our focus has been more on the market players, such issues are just touched on, although more discussed in the social assessment part.

There are also a number of other issues that resides in or in-between the economic and social assessments, for example the impact and value of knowledge creation to the society and impact on employment (new jobs). Indeed, the methods for economic assessment listed in section 2.1 indicate the range and complexity of both issues that are potentially raised when conducting an economic assessment:

- Input-output method: typically used to assess ripple effects and job creation potential
- CGE: useful for assessing policy instruments such as taxes, subsidies or command-and-control policies.

None of these are used for this assessment. In order to carry out an input/output analysis, the effect of the tools on end users demand and the industry interdependencies must have been well understood and quantified. CGE models are typically, highly aggregated and designed for assessment of policies, not concrete ICT tools. With the present knowledge of for example the market acceptance of the tools neither the Input-output method, nor the CGE models are well suited for the economic assessment.

9.5.1 Interview methodology

For the interviews, we recruited companies and organizations that differed in their role in the cloud value chain, and in their organizational nature. We recruited both public organizations and private companies. Most were large, with more than a thousand employees. We decided to approach companies we knew were interested in the topic, and that we had previous contact with. To reduce the effort for them to participate – and hence get a larger possibility of accepting an interview – we decided to perform all interviews at their locations wherever possible. The subjects were offered anonymity to encourage them to express their views freely. One exception is Hewlett Packard Enterprise who we disclose because Hewlett Packard's central role in the A4coud consortium.

SINTEF invited a total of seven companies and institutions for interviews. Five of them responded positively and interviews were scheduled. One did not respond at all to the requests, while one responded positively, but was unable to go through with the actual interview.

The four interviews were performed at their locations included two or three researchers. One researcher had a more technical background and kept the conversation flowing on technical issues of the A4Cloud tools and cloud challenges. The others were in charge of using the interview guidelines,

and took notes. One interview was conducted via phone. In this interview we decided to only use one researcher. Each interview lasted between 60 and 90 minutes.

The companies met with between one and three respondents. They were encouraged to participate with more than one person if they had the opportunity so that we could have as much information available as possible.

9.5.2 Description of participants

The University

The university we interviewed is one of the three largest in Norway. Their IT support department has three main tasks: running collective and basic services for the employees and students, developing web-based solutions for the university, and advising the university regarding IT-related questions. The university identified themselves as primarily a cloud customer. We talked to the head of the IT support department and a procurement officer.

The research foundation

The research foundation is one of the top three in Norway according to their number of employees. Their IT network is delivered by an external partner, while operations and support is maintained by another external partner. The research foundation employs a handful of people that make decisions on security issues, use and purchase of IT services, allowed equipment etc. They operate some cloud services, but participated in the interview with the perspective of a cloud customer. We talked to the head of IT security.

The Local Government

The local government operates at the municipality level and is one of the top three largest cities in Norway. Their IT section has around 40 employees, six of which are currently involved in the purchases and use of cloud services for the municipality. They have recently decided to start using Google Apps for Education in all schools in their area and thought of themselves as a cloud customer. We talked to a project manager who was responsible for procurement and implementation of cloud services.

The Network Provider

The network provider develops and operates the national research and education network. They also deal with identity management, purchase co-operation, network management and security for their customers. They described themselves as a broker for cloud services. We talked to a business developer and a highly experienced project manager involved with developing cloud services tools.

Hewlett Packard Enterprise

Hewlett Packard Enterprise is a world leading provider of cloud services. We interviewed the director of strategy and solutions for Hewlett Packard Enterprise Services worldwide Financial Services Industry go to market organisation. The subject has no other involvement in the A4cloud project.

9.6 Appendix Security Threat analysis methodology

9.6.1 Data Track

Threat Model Information:

Threat Model ID	TM.1
Tool Name	Data Track (DT)
Description	The DT is a tool that gives data subjects an overview of all the personal data they have disclosed. This tool allows them to search through their data disclosure history. They can see what personal data they have disclosed, to whom and under which privacy policy.

Dependencies:

ID	Name	Description
D1.1	Transparency Log	A4Cloud tool

D1.2	APPLE	A4Cloud tool
D1.3	Javascript libraries	Used in DT Frontend
D1.4	Data persistency	Based on SQLite

Entry Points:

ID	Name	Description
E1.1	DT API	Public API offered by Data Track
E1.2	DT Frontend	User interface
E1.3	DT Local storage	SQLite database for storing persistent data
E1.4	TL Plugin	Plug-in for communicating with TL

Assets:

ID	Name	Description
A1.1	Data disclosures	Information that is disclosed to external parties

Trust Levels:

ID	Name	Description
L1.1	Data subject	The only user of Data Track is the data subject

Threats:

ID	Name	STRIDE	Vulnerable point
T1.1	Attacker may impersonate data subject through DT Frontend	Spoofing	DT Frontend
T1.2	Attacker may tamper with encrypted data in DT Local Storage	Tampering	DT Local storage
T1.3	Attacker may tamper with DT communications	Tampering	DT communications
T1.4	Attacker can perform actions without being logged	Repudiation	DT Frontend, DT API
T1.5	Attacker may access encrypted DT Local Storage	Information disclosure	DT Local storage
T1.6	Attacker may read DT communications	Information disclosure	DT communications

9.6.2 Transparency Log

Threat Model Information:

Threat Model ID	TM.2
Tool Name	Transparency Log (TL)
Description	TL provides a secure and privacy-preserving one-way communication channel between service providers and data subjects. Using TL, service providers can share more data with data subjects, including potentially privacy-sensitive data, which normally cannot be sent via for example email or SMS.

Dependencies:

ID	Name	Description

D2.1	Data persistency	Bolt database
D2.2	Secure communications	TLS protocol
D2.3	Anonymous communications	Tor protocol

Entry Points

ID	Name	Description
E2.1	TL Sender	API to users' piles
E2.2	TL Recipient	API for receiving messages/events
E2.3	TL Sender Local Storage	Stored data at Sender side

Assets:

ID	Name	Description
A2.1	TL Sender Local Storage	Event piles

Trust Levels:

ID	Name	Description
L2.1	TL Sender public	TL Sender has some public APIs
L2.2	TL Sender private	TL Sender has private APIs, intended only for the sender
L2.3	TL Recipient	TL Recipient APIs

Threats:

ID	Name	STRIDE	Vulnerable point
T2.1	Attacker may impersonate TL Sender using his credentials	Spoofing	TL Sender private credentials
T2.2	Attacker may impersonate TL Receiver using his credentials	Spoofing	TL Receiver credentials
T2.3	Attacker may saturate TL Sender service	Denial of Service	TL Sender service

9.6.3 Audit Agent System

Threat Model Information

Threat Model ID	TM.3
Tool Name	Audit Agent System (AAS)
Description	The AAS is a tool for auditors and providers to use to verify the compliance with policies. It automatically and continuously collects and analyses evidence, and assures accountable execution of processes in the cloud.

Dependencies

ID	Name	Description
D3.1	IMT	Incident Management Tool
D3.2	TL	Transparency Log
D3.3	APPLE	Policy Engine
D3.4	Java JRE	Java Runtime Environment
D3.5	JADE	Multi Agent framework for Java
D3.6	Jetty	Web Server

D3.7	Apache HTTP Server	Web Server

Entry Points

ID	Name	Description
E3.1	AAS API	Public API offered by AAS
E3.2	AAS Frontend	User interface
E3.3	Evidence Store	Repository of evidence records
E3.4	AAS Collector Agent interfaces	Input to audit agents

Assets:

ID	Name	Description
A3.1	Evidence Store	Repository of evidence records

Trust Levels:

ID	Name	Description
L3.1	Auditor	The only intended user of AAS is an auditor

Threats:

ID	Name	STRIDE	Vulnerable point
T3.1	Attacker may impersonate auditor through AAS Frontend	Spoofing	AAS Frontend
T3.2	Attacker may tamper with AAS communications (e.g., agents)	Tampering	AAS Communications
T3.3	Attacker may access encrypted Evidence Store	Information disclosure	Evidence Store
T3.4	Attacker may read AAS communications (agents)	Information disclosure	AAS Communications
T3.5	Attacker may saturate Evidence Store server (e.g., acting as agents)	Denial of Service	Evidence Store
T3.6	Attacker can perform actions without being logged	Repudiation	AAS Frontend

9.6.4 Incident Management Tool

Threat Model Information:

Threat Model ID	TM.4
Tool Name	Incident Management Tool (IMT)
Description	The IMT is the entry point for handling anomalies and detected violations in cloud environment scenarios. This tool receives incident notifications from downstream providers or local A4Cloud tools, such as AAS. It also notifies upstream providers of incidents. In cases where incidents received by IMT affect end-users of this provider, IMT takes the initial steps to respond to these incidents by sending alerts. The IMT and RRT are linked.

Dependencies:

ID	Name	Description
D4.1	APPLE	Policy Engine
D4.2	Web server	Unspecified web server (probably Tomcat/Apache)

Entry Points:

ID	Name	Description
E4.1	IMT API	Public API to IMT
E4.2	IMT Frontend	User interface

Assets:

ID	Name	Description
	none	

Trust Levels:

ID	Name	Description
L4.1	Auditor	The only intended user of IMT is a Cloud Auditor

Threats:

ID	Name	STRIDE	Vulnerable point
T4.1	Attacker may impersonate auditor through IMT Frontend	Spoofing	IMT Frontend
T4.2	Attacker can perform actions without being logged	Repudiation	IMT Frontend
T4.3	Attacker may saturate IMT server	Denial of Service	IMT Server

9.6.5 Data Protection Impact Assessment Tool

Threat Model Information:

Threat Model ID	TM.5
Tool Name	Data Protection Impact Assessment Tool (DPIAT)
Description	The DPIA tool has a friendly web-based interface. It presents 2 questionnaires about the data protection measures for a given project: an initial screening and a subsequent full screening. These questionnaires are tailored to the needs of Small and Medium Enterprises (SMEs). The approach is based on legal and socio-economic analysis of privacy issues for cloud deployments and takes into consideration the proposed new requirements for DPIAs within the European Union (EU).

Dependencies:

ID	Name	Description
D5.1	Web server	Unspecified web server (probably Tomcat/Apache)

Entry Points:

ID	Name	Description
E5.1	DPIAT Frontend	User interface

Assets:

ID	Name	Description
A5.1	User environment questionnaires	Contains information regarding the company or organization of the user

Trust Levels:

ID	Name	Description
L5.1	Cloud customer	

Threats:

ID	Name	STRIDE	Vulnerable point
T5.1	Attacker may read customer details	Information disclosure	
T5.2	Attacker may saturate DPIAT server	Denial of service	DPIAT Server

9.6.6 Data Protection Policies Tool

Threat Model Information:

Threat Model ID	TM.6
Tool Name	Data Protection Policies Tool (DPPT)
Description	The DPPT facilitates the joint specification and implementation of accountability policies between cloud customers and cloud providers/brokers/carriers. It creates a machine readable privacy policy and a technical representation of the policy that allows for (automatic) policy enforcement of data protection.

Dependencies:

ID	Name	Description
D6.1	Web server	Unspecified web server (probably Tomcat/Apache)
D6.2	APPLE	A4Cloud tool

Entry Points:

ID	Name	Description
E6.1	DPPT Frontend	User interface

Assets:

ID	Name	Description
A6.1	Policies	APPLE policies

Trust Levels:

ID	Name	Description
L6.1	Privacy administrator	Belongs to the Cloud Provider

Threats:

ID	Name	STRIDE	Vulnerable point
T6.1	Attacker may impersonate privacy administrator through DPPT Frontend	Spoofing	DPPT Frontend
T6.2	Attacker can perform actions without being logged	Repudiation	DPPT Frontend
T6.3	Attacker may saturate server	Denial of	DPPT Server

		service	

9.6.7 Redress and Remediation Tool

Threat Model Information:

Threat Model ID	TM.7
Tool Name	Redress and Remediation Tool (RRT)
Description	The RRT assists individual end users or small SME cloud customers in responding to (perceived) incidents in their cloud arrangements. The RRT is activated when certain incidents are reported by the Incident Management Tool (see previous description) or when it is invoked by the users on the basis of information collected from other sources. It lists possible actions that can be undertaken and will guide users through the actions.

Dependencies:

ID	Name	Description
D7.1	Web server	Unspecified web server (probably Tomcat/Apache)
D7.2	Data Track	A4Cloud tool
D7.3	IMT	A4Cloud tool

Entry Points:

ID	Name	Description
E7.1	RRT Frontend	User interface
E7.2	RRT API	Public API

Assets:

ID	Name	Description
	none	

Trust Levels:

ID	Name	Description
L7.1	Data subject	

Threats:

ID	Name	STRIDE	Vulnerable point
T7.1	Attacker may impersonate data subject through DT Frontend	Spoofing	RRT Frontend
T7.2	Attacker may saturate server	Denial of service	RRT Server

10 Index of figures

11 Index of tables